# *States Confront the Cyber Challenge*

**Memo on State Cybersecurity Strategies**

## *General Overview*

This memo provides an overview of state cybersecurity strategies, as well as information technology and homeland security strategies with cybersecurity components. Possessing and implementing a cybersecurity strategy is critical for the state and assists in garnering more resources.[1] Through this overview, NGA has identified a number of best practices for states considering developing a statewide cybersecurity strategy.[2] Among the 22 plans identified in 18 states, 14 are IT strategic plans, six are cybersecurity strategic plans, and two are homeland security strategic plans. The IT and homeland security agencies' strategic plans tend to limit their scope to primarily protecting the state's IT ecosystem and critical infrastructure, respectively. The statewide cybersecurity strategic plans, however, detail specific objectives to achieve a wide range of goals.

Nonetheless, there were recurring goals throughout all the plans: protecting state's IT infrastructure and data; developing and exercising a cyber response plan to protect critical infrastructure; training employees on cyber hygiene; improving the cybersecurity workforce talent pool; creating a governance structure and metrics; and creating partnerships. The following section highlights states with innovative goals and objectives within these areas.

## *Best Practices*

Model plans identify protecting IT infrastructure as a key goal, and, for most states, the first step to achieving this is to move from a compliance-based approach to a risk-based approach. The benefit of a risk-based approach is that a state tailors their priorities to the vulnerabilities of their most critical assets, while a compliance-based approach focuses on "checking-off" a list of actions a state should do, regardless of their needs. Furthermore, conducting risk assessments to identify strengths and weaknesses assists in creating a comprehensive cybersecurity strategy. **Iowa**, for example, plans on creating an operational plan, timeline, and budget that addresses gaps and prioritizes remediation once they measure their cyber risk. Another state, whose strategy is not public, uses scorecards to measure the maturity of security controls within state agencies and their risk to threats.

Risk assessments can also inform cyber incident and disruption plans by identifying vulnerable systems and supplying information needed to prioritize response efforts. Creating, formalizing, and improving these response plans are goals or objectives in 12 states, and **Wisconsin** dedicated an entire strategic plan to creating a cyber disruption plan. **Maryland's** homeland security strategy details several objectives to establishing a disruption plan, such as

[1] Deloitte and the National Association of State Chief Information Officers. "2016 Deloitte-NASCIO Cybersecurity Study." http://www.nascio.org/Portals/0/Publications/Documents/2016/2016-Deloitte-NASCIO-Cybersecurity-Study.pdf

[2] All plans were collected in September 2016.

coordinating state agencies' network protection plans to meet a minimum standard, and inventorying public and private infrastructure to produce a system for securing targets of interest.

One of the top priorities among state chief information security officers is to train and raise awareness among state employees who lack basic cyber hygiene and are susceptible to malicious cyber activity.[3] Therefore, states should consider integrating employee cyber hygiene training into their plan to further mitigate cyber risks. For example, **Iowa's** plan requires cybersecurity awareness training for all state employees and to measure the effectiveness of the training. Similarly, several states are keenly aware of the cybersecurity workforce deficit and recognize the need to groom the future cybersecurity workforce. For instance, **Michigan** plans to promote cybersecurity careers to high school students, encourage the improvement of cybersecurity occupational certification programs, and work with academia and private sector partners to determine new workforce requirements.

To coordinate these goals, a few states have recognized a need to create a governance structure. **Florida**, for example, intends on establishing a cybersecurity governance structure and using working groups to create the state's cybersecurity framework and to inventory their current enterprise architecture. Some states have taken an informal approach to measuring their cybersecurity strategy, such as establishing metrics and creating accreditation programs for software purchases across state agencies. Lastly, these plans seek to promote partnerships with other public, private, and federal entities. **West Virginia's** plan is notable in that it calls on the state to provide cybersecurity awareness training to local governments.

**Conclusion**

A risk-based strategy that identifies a state's current threats, vulnerabilities, and capacity to defend prized assets provides a governor with the information he or she needs to enact measures that protect the state from cyber threats. Additionally, a strategy with metrics and methods of evaluation ensures that a strategy's objectives are achieving their stated goals. As a result, a governor could prioritize and justify cybersecurity investments in key areas based on validated metrics. Lastly, enlisting metrics ensures that a strategic plan is a living document that can be updated as needed.

The following pages highlight the 22 plans' goals and objectives. Please see "6 Steps to a Cyber Strategy" for a template process on creating a cybersecurity strategic plan.

*Please e-mail Michael Garcia, Policy Analyst, Homeland Security and Public Safety Division, NGA at:* mgarcia@nga.org *with any questions.*

[3] Deloitte and the National Association of State Chief Information Officers. "2016 Deloitte-NASCIO Cybersecurity Study." http://www.nascio.org/Portals/0/Publications/Documents/2016/2016-Deloitte-NASCIO-Cybersecurity-Study.pdf

**CA, Information Technology Strategic Plan, 2016 (5 Objectives, 18 Strategies)**

- Protect sensitive data through robust security and privacy programs
  - Implement and monitor compliance with security and privacy policies, standards, and practices.
  - Provide accountability where compliance failure has exposed sensitive data to avoidable risk
  - Raise awareness of information security risks and educate and train state technology users.
  - Implement next-generation security tools.
- Ensure the state's technology and public safety communication infrastructures have robust and reliable disaster recovery capabilities to support the continuity of government services
- Improve how California uses public data and information by encouraging and enabling shared capabilities, promoting transparency, and increasing the availability of relevant, accurate, and useful data to constituents and to public sector entities
  - Use data management and collaboration tools to increase the ease of data analysis to leverage better value from the data collected by departments.
  - Collect and share lessons learned from state agencies.
- Ensure California's IT workforce has the knowledge and skills to support the state's technology infrastructure and implement its technology vision
  - Attract a skilled workforce by analyzing and evaluating current and future technology skillset needs, and implement outreach, recruitment, and knowledge transfer strategies.
  - Partner with the department of human resources to modernize IT classifications, recruitment, and hiring.
  - Maintain a skilled workforce by developing the capabilities of employees to fill leadership positions and other key critical positions requiring specialized knowledge.
  - Expand educational opportunities to develop core competencies of employees in IT functional areas such as cyber security, service desk management, software development, infrastructure, and project management.
  - Grow the project academy series to build out full day training offerings to educate IT project teams, project sponsors, and stakeholders on IT project best practices, lessons learned, and project leadership.
  - Establish communities of interest to share IT project methodologies and expertise, and share best practices.
  - Ensure the IT community has access to experienced project management staff and consulting services.
  - Provide expertise and training for the successful completion of all phases of the project lifecycle from concept to completion.
  - Expand partnerships with the public and private sectors to deliver educational conferences based on technology trends and best practices.
  - Foster support of on-the-job training for legacy technologies no longer taught in the universities (e.g., mainframe).
- Recognize success and excellent service by state employees and departments in order to foster a sense of accomplishment and accountability for the state's workforce
  - Recognize state IT staff for their achievements at the quarterly agency information and chief information officer meetings and at conferences.

- Ensure state entities are informed of opportunities that recognize the good work that is completed in California which include the National Association of State Chief Information Officers (NASCIO), Best of California, etc.

## CO, Strategy for Information Security and Risk Management, 2016-2018 (4 Goals, 18 Strategic Initiatives)

- Protect state information and information systems to assure that the confidentiality, integrity, and availability of all information is commensurate with mission needs, information value, and associated threats.
  - Design, build, and operate resilient and self-healing systems and networks that are capable of resisting current and emerging cybersecurity threats
  - Recruit, develop, and retain a motivated, professional, and knowledgeable information security workforce
  - Design, build, and operate the necessary tools, techniques, and procedures to maintain "24/7" information security situational awareness of all state networks, systems, and data
  - Develop and maintain information security policies, standards, and guidelines that are relevant, adaptable, and cost-effective
  - Promote the understanding and acceptance of information security concepts and practices throughout state government.
  - Equip state information technology professionals with the tools, knowledge, and skills to design, build, and operate secure applications and systems
  - Develop, document, and socialize an information security architecture that (1) aligns with the technology strategy, (2) transparently integrates security processes into next-generation state networks and systems, and (3) anticipates and addresses future threats
  - Develop and maintain a statewide incident response and computer forensic capability that is able to (1) quickly identify and isolate security incidents, (2) recover impacted systems and business processes, and (3) when feasible, identify and prosecute those attacking state systems
  - Develop, document, and implement a standardized risk management framework for accurately and uniformly assessing and managing the risk to the confidentiality, integrity, and availability of state systems and networks
- Research, develop, and employ innovative and sustainable information security solutions to address Colorado's cyber security challenges.
  - Actively leverage federal government, private sector, academic research, and development of advanced cyber security tools and capabilities to assure the confidentiality, integrity, and availability of state systems and data
  - Rapidly evaluate, build, and deploy cutting-edge information security technologies to outpace emerging threats
  - Identify, evaluate, and share information on the threats and vulnerabilities impacting state government to support future research and development efforts
- Develop and foster key partnerships to improve information sharing, reduce information security risks, and to promote innovation and collaboration.
  - Develop and formalize new partnerships with academic institutions, the private sector, and Colorado's state and local governments to share information security threat intelligence, research and development efforts, and best practices
  - Maintain active participation with the relevant organizations such as the National Association of State Chief Information Officers' (NASCIO) Privacy and Security Committee, Multi-State Information Sharing Analysis Center (MS-ISAC), and the SANS Institute

    - Promote discussions and cooperative engagements that will enhance cyber security for all Colorado residents including partnering with the department of public safety in achieving the cyber security objectives of the division of homeland security and emergency management strategy
- Comply with applicable information security and data privacy laws and regulations.
    - Continuously assess and evaluate state systems and networks
    - Conduct targeted, technical audits to identify and correct non-compliance with state information security policies and applicable federal laws and regulations
    - Partner with executive branch agencies to assist them in preparing for and responding to information security-related audits.

**DE, Statewide Information Technology Strategic Plan, 2016-20149 (1 Objective, 4 Focuses, 10 Strategies)**

- Reliable, Secure, and Resilient Services
    - Establish the Delaware Cyber Security Advisory Council
        - Develop best practices to mitigate cyber security risks
        - Improve overall security posture across all sectors in Delaware
        - Increase information sharing between all sectors in Delaware
    - Promulgate the Delaware Emergency Operations Plan
        - Establish disruption response plans for all agencies supported through centralization
        - Conduct drills to test, evaluate, and modify plans annually
    - Improve the overall security posture
        - Provide backup and recovery of critical system
        - Provide fail over services for mission critical services
        - Provide planning, testing, and readiness assessments
        - Provide enterprise network security monitoring and vulnerability scanning
    - Deliver education and awareness
        - Improve existing and develop new internal and external programs

**FL, 2015-2018 Statewide Strategic Information Technology Security Plan (3 Strategies, 7 Objectives)**

- Enhance security and privacy capabilities
    - Implement a cybersecurity framework
    - Improve situational awareness
    - Develop a robust enterprise security incident response program
- Enhance the enterprise IT environment
    - Invest in core enterprise enhancement
    - Develop and implement application rationalization process
- Define the roadmap for maturing IT processes and strategic business alignment
    - Strengthen project assurance and ensure project oversight
    - Coordinate multi-agency enterprise initiatives

**IA, Cybersecurity Strategy, 2016 (9 Goals, 31 Recommendations)**

- Protecting lifeline critical infrastructure: Address high risk cybersecurity areas for the state's critical infrastructure and develop plans to better identify, protect, detect, respond, and recover from significant cyber incidents.
    - Implement the National Cybersecurity Framework to create a baseline for measuring cybersecurity risk and assessing progress in lifeline critical infrastructure services and state government.

    - Formalize the cybersecurity incident response plan and necessary agreements and processes for collaboration between state agencies, and regularly exercise the plan
    - Continue forging partnerships with lifeline critical infrastructure sectors to ensure the resiliency of digital systems. Promote and facilitate joint training and exercise scenarios
    - Promote additional public and private assessment processes such as the HSEMD/ US-DHS Critical Infrastructure IP Gateway Survey Program and the utilities board cyber reviews
    - Leverage state resources, such as the Iowa Communications Network pursuant to IAC 8D.9 (3) to test, secure and protect critical communication infrastructure
- Risk Assessment: Establish a process to regularly assess cybersecurity infrastructure and activities within the State.
    - Report annually to the governor's office and legislature on the current state of cybersecurity risk, COOP/COG, and IT disaster recovery readiness for the executive branch
    - Assemble a working group of public and private subject matter experts to evaluate the current risk assessment process and make specific recommendations for improving the overall process.
    - Improve accountability and transparency of state government's cybersecurity posture by creating a cybersecurity risk assessment report card.
- Best Practices: Provide recommendations related to securing networks, systems, and data, including interoperability, standardized plans and procedures, and evolving threats and best practices to prevent the unauthorized access, theft, alteration, and destructions of data held by the State of Iowa.
    - Fully implement the CIS-CS Controls for Effective Cyber Defense
    - Leverage the findings from the 2016 Executive Branch Cybersecurity Survey and create an operational plan, timeline and budget which addresses gaps and prioritizes remediation within the CIS-CS and National Cybersecurity Security Framework
    - Reduce duplicative security products and initiatives and consolidate resources and solutions under the OCIO
- Awareness Training: Implement cybersecurity awareness training for state government
    - Require general cybersecurity awareness training for all State of Iowa employees and additional specialized cybersecurity awareness training for employees with privileged access. Conduct regular testing to measure the overall effectiveness of the training.
    - Further educate the state's leadership on cybersecurity risk and their roles and responsibilities
    - Create a cybersecurity training environment to facilitate cross agency training
- Public Education and Communication: Identify opportunities to educate the public on ways to prevent cybersecurity attacks and protect the public's personal information
    - Institute a public cybersecurity awareness and literacy campaign to improve the cybersecurity awareness of Iowans and promote good cyber hygiene
    - Facilitate and sponsor an annual public and private cybersecurity conference
    - Provide cybersecurity awareness and literacy curricula and support materials for K-12 and college students
- Collaboration: Collaborate with the private sector and educational institutions to implement cybersecurity best practices.
    - Improve and enhance current partnerships with educational institutions to identify cybersecurity best practices through internships and faculty expertise

    - Conduct cybersecurity training exercises across Executive Branch agencies and lifeline critical infrastructure sector partners
    - Identify, create, review and update legal agreements between collaborative partners to improve information sharing, preparedness and incident response
    - Expand private sector partnership programs to promote the sharing of criminal and cyber-threat information affecting the private sector in Iowa
- STEM: Recommend science, technology, engineering, and math (STEM) educational and training programs for K-12 and higher educational programs in order to foster an improved cybersecurity workforce pipeline
    - Incentivize students to pursue careers in cybersecurity through the creation of scholarship programs modeled after programs such as the Federal Cyber Corps; Scholarship for Service program, the AmeriCorps Model, the Military GI Bill, and others
    - Provide and encourage pathways to cybersecurity careers from K-12 through higher education
    - Conduct a review of the cybersecurity workforce requirements for the executive branch and recommend necessary adjustments
- Data Breach: Establish data breach reporting and notification requirements
    - Work with the attorney general to introduce changes to Iowa's Code Chapter 715C which would facilitate greater insight into the security breaches occurring in the state and better protect the personal information of the citizens of Iowa
    - Participate in initiatives designed to standardize data breach notification requirements at a national level to aid in the protection of citizen privacy and establish consolidated standards and reporting.
    - Track and report the data breach impact to citizens of Iowa and Iowa businesses
- Emergency Response Plan – Cyber Annex: The homeland security and emergency management department shall update the state's emergency response plan to deal with the physical consequences of a significant cyberattack against the State's critical infrastructure
    - Develop a strategic direction on how the state prepares and responds when cyber-incidents involving lifeline critical infrastructure or state government escalate to a level of significance requiring a coordinated response from a state and/or HSEMD perspective
    - Define a process to manage significant cyber incidents and provide a basis for continuing refinement of our processes and policies that address the path from steady-state to incident response
    - Formalize the cyber annex of the emergency response plan and the cyber incident response plan with required reviews and updates every two years
    - Exercise the cyber annex as part of the emergency response plan and the cyber incident response plan

**ID, State Government Technology Strategic Plan, 2016 (2 Goals, 2 Objectives, and 8 Strategies)**

- Manage IT and information from the perspective of state government as a whole
    - To provide infrastructure and managed services for data, voice and video that are secure and available, properly scaled and distributed with universal connectivity throughout the state in a cost-effective manner.
        - Confirm completion of 2014 objectives
        - Assess network for: cloud performance issues, network redundancy, segmented networks, review network security, and develop user standards
        - Define benefits of the investment

        - Long-term network contract
- Safeguard the security, confidentiality, integrity and availability of information
    - To implement cybersecurity best practices in order to help manage cybersecurity risk and maintain the integrity of state information.
        - Adopt NIST framework
        - Training for all employees
        - Metrics to show vulnerabilities and progress
        - Document benefits to the governor for funding.

**KY, The Commonwealth Office of Technology Strategic Plan, 2014-2018 (2 Objectives, 9 Strategies)**

- To enhance and continually improve IT security
    - Implement appropriate security policies based on NIST
    - Formalize the annual commonwealth cyber security exercise and incorporate lessons learned and recommendations from each exercise into the lessons learned and recommendations from each exercise into the appropriate polices, standards, and procedures
    - Constantly evaluate and enhance security toolsets and services
    - Conduct a review of compliance with the roadmap for enterprise security and provide guidance to agencies
    - Review, update, and continue implementing the roadmap for enterprise security
- To raise awareness of the significance of security threats and vulnerabilities
    - Assess agencies based on security awareness and make results available to agency leaders
    - Create and distribute a series of quarterly security reports to agency leadership and the governor's cabinet
    - Complete, track, and evaluate effectiveness of COT's internal security awareness training
    - Evaluate annual security awareness initiative to increase business unit participation

**MA, State Homeland Security Strategy, 2014 (1 Goal, 1 Objective, 6 Strategies)**

- Protect the commonwealth from intentional acts of violence and terrorism
    - Enhance the security of cyber systems by protecting against damage to, unauthorized use of, and/or the exploitation of electronic communications systems and services
        - Develop specific cyber disruption plans
        - Assess cyber disruption threat across the commonwealth
        - Enhance training with emphasis on cyber systems and disruption
        - Promote private/public partnerships around cybersecurity and disruption
        - Continue to evaluate cyber-related risk, vulnerability, and capability assessments for high priority buildings, systems and technical capabilities across the commonwealth
        - Harden access control of publicly owned network and infrastructure.

**MA, Office of Information Technology Strategic Priorities, 2017 (1 Priority, 3 Objectives)**

- Security: Better protect information entrusted to us, while providing appropriate access
    - Strengthen security governance and clarify roles and responsibilities
    - Shift focus from compliance and documentation to action and responsiveness
    - Improve visibility and intelligence into ever-increasing risks and threats

## MD, Statewide IT Master Plan, 2017 (1 Objective, 5 Strategies)

- Cybersecurity Policies and Programs
  - Establishing a governance and authority structure for cybersecurity;
  - Conducting risk assessments and allocating resources accordingly;
  - Implementing continuous vulnerability assessments and threat mitigation practices;
  - Complying with current security methodologies and business disciplines in cybersecurity;
  - Creating a culture of risk awareness.

## Maryland Governor's Office of Homeland Security Initiatives and Priorities (1 Objective, 4 Goals, 11 strategies)

- Core Goal 6: Cyber Security and Critical Infrastructure Protection
  - All state government computer networks and systems should be protected from cyber attacks and regularly tested for security and safety
    - Coordinate individual state agency network protection plans so that each agency meets a minimum protection standard, addresses physical and electronic assets, and includes an annual security self-audit.
    - Lead regular training for state agency CIOs and develop network safety and provide security training materials for the state's workforce.
    - Collect reports of cyber attacks or incidents against state agency networks and create a process to share information with the appropriate IT and public safety stakeholders in a timely manner.
    - Conduct random data security compliance assessments for selected agencies throughout the year and, where applicable, include the results of such assessments in agency self-audit reports.
  - Critical private sector entities including utilities should be included in cyber security planning, training, and exercising
    - Identify private sector networks critical to the operations of the state's information technology infrastructure and share and implement cyber security solutions including both technological solutions and training and education of personnel.
    - Share alerts and notifications of potential cyber threats with trusted private sector partners
  - Maryland should be able to effectively respond to cyber incidents involving public and private networks that affect the well-being of Maryland residents, businesses, and the ability of the state to provide essential government services
    - Develop a cyber incident response plan to coordinate federal, state, local, and private sector activities and manage the risks associated with an attack or malfunction of critical information technology systems within the State.
    - Ensure all state agencies' continuity of operations (COOP) plans include alternate methods of business operations for systems that may be affected by a cyber incident
  - Maryland should have a complete and prioritized inventory of critical infrastructure, including assets controlled by the private sector, and a system for securing high-priority targets or populations of interest.
    - Develop a single, shared database of critical infrastructure, map all qualifying assets, and overlay suspicious activity reports (SARs) to identify patterns and proximity to critical infrastructure.

- Create a platform to disseminate alerts and notifications regarding threat intelligence and emergency incidents to critical infrastructure owners and operators.
- Prioritize critical infrastructure assets and conduct on-site physical security assessments at high-risk facilities and sites.

## MI, Cyber Initiative, 2015 (3 Objectives, 26 Strategies)

- Leadership, Prevention, Detection, Response
  - Further develop partnerships within the cybersecurity ecosystem to take the cyber disruption plan to the next level, including establishing the cyber defense response team to support state government and key stakeholders in the state during and after a cyber event
  - Conduct annual cybersecurity exercises to further prepare state governments and private entities to respond in the event of a cyber disruption
  - Continue to update the foundational elements of cybersecurity in the state to adhere to the NIST Cybersecurity Framework
  - Move closer to full implementation of a cybersecurity architecture based on the zero-trust security model
  - Transition from a compliance-centric approach to cybersecurity to a risk-based approach
  - Partner with leading cybersecurity experts to develop a practical cyber risk model
  - Work with public and private organizations to develop draft legislation to allow for this necessary information sharing that can serve as a model for other states
- Education and Public Awareness
  - Continue to offer leading edge training and awareness programs, enhance the Michigan Cyber Range to include more sites and courses, and offer exciting cyber summits and roadshows around the state
  - Expand education efforts to target P-20 students with online and classroom training
  - Hold town hall meetings with intermediate school districts throughout the state to offer support to enhance cybersecurity awareness programs in schools
  - Follow the National Initiative for Cybersecurity Education Framework
  - Continue the deployment of Michigan Cyber Range extension sites at National Guard bases
  - Roll out a free IT security assessment tool, CySAFE, to help small and mid-sized governments assess, understand, and prioritize their basic IT security needs
  - With our public and private partners, develop cyber-threat warning levels that provide the public with threat awareness information in real time
- Michigan's Unique Cyber Industry Opportunity
  - Encourage public and private collaborations to utilize the DHS cybersecurity competency framework
  - Work with academia and industry to determine new workforce requirements from emerging technology and threats
  - Promote the Michigan Cyber Range as a valuable resource to enable industry and IT specialists to develop advanced cybersecurity skills and certifications
  - Encourage the improvement and advancement of cybersecurity occupational certification programs
  - Establish a baseline for cybersecurity professionals across multiple industry sectors
  - Encourage the establishment of a professional organization to provide education, training and networking opportunities

- Promote employment opportunities and feature employers through talent information newsletters
- Work closely with employers to match talent to their needs
- Promote cybersecurity careers to high school students, connecting them to post-secondary training programs
- Expand existing international, regional and local economic development partnerships
- Facilitate the convergence of cybersecurity with key industries
- Facilitate the launch of industry specific "Cybersecurity Technology Innovation Challenges"

**MN, Master Plan, Information and Telecommunications, 2012-2017 (4 Strategies, 14 Objectives)**

- Continue developing core enterprise security program functions that will help proactively manage information security risk
  - Continue movement towards an enterprise security model that coordinates all planning, oversight, and response activities through a single program.
  - Adopt processes to design appropriate security controls in new systems or systems that are undergoing substantial redesign.
  - Provide employees at all levels with relevant security information and training to lessen the number of security incidents
  - Build a compliance program to validate that information security controls are functioning as intended
  - Improve boundary defenses by installing a zoned security model that separates and controls access to different networks with different threat levels.
  - Adopt a hardened security defense model for computers that routinely interact with untrusted devices on the internet or may be prone to loss or theft
  - Develop central processes and tools to manage physical and logical access to state computer systems and data more efficiently and effectively
- Continue developing enterprise-wide information security processes and tools to improve situational awareness
  - Gain better situational awareness through continuous monitoring of networks and other IT assets for signs of attack, anomalies, and inappropriate activities.
  - Continuously identify and remediate vulnerabilities in state computer systems before they can be exploited.
- Continue developing shared processes to minimize the impact of adverse security events
  - Increase emphasis on business continuity planning and disaster recovery testing across all agencies and all systems
  - Provide centralized security incident response and forensic investigation services to determine the cause, scope, and impact of incidents and limit damage.
- Minimize risk and maximize redundancy in major systems and facilities
  - Reset and accelerate data center virtualization and consolidation to achieve an acceptable risk level for the data and systems that manage state operations; partner with other state government entities to develop and leverage shared data center strategies
  - Encourage adoption of the state's high-security network, communications and collaboration tools among all branches of state and local government to increase security inter-government communications and interoperability.

**MS, Strategic Master Plan for Information Technology, 2016-2018 (1 Strategy, 10 Actions)**

- Provide, protect, and support enterprise technology infrastructure components to strengthen the security posture of the state
    - Align enterprise security policies, standards, plans, and other cybersecurity documents with current security methodologies and industry standards, such as the NIST Cybersecurity Framework
    - Coordinate the state's participation in Cyber Storm V
    - Develop an enterprise incident response plan
    - Research the cybersecurity insurance market for available coverage to mitigate losses from a variety of cyber incidents
    - Research secure web gateway solutions to enhance the ability to protect state assets against attacks by detecting and filtering unwanted software and malicious code from user initiated Internet traffic
    - Research next-generation firewall technologies
    - Research virtual private network (VPN) technologies
    - Implement a managed security service log correlation solution
    - Manage and enhance security vulnerability management tools and leverage internal/external partners
    - Perform, coordinate, and promote security education, awareness and cyber exercises

**MT, State Information Technology Services Division 2016 (1 Goal, 4 Objectives)**

- Manage Cybersecurity Risk to Systems, Assets and Data
    - Develop best practices for common security controls for all agencies to use
    - Develop and implement a standardized information security program assessment and measures for departments and the state
    - Provide a yearly state information security assessment to the governor showing program successes and a plan to address shortcomings
    - Develop a governor's information security dashboard

**NC Planning and Financing State Information Technology Resources for the 2015-2017 Biennium (1 Goal, 4 Objectives, 10 Initiatives)**

- Modernize and Secure IT Systems
    - Standardize and improve office of information technology (OIT) service deliver
        - Conduct a comprehensive service assessment
        - Develop a new service catalog
    - Enhance the agility of our infrastructure
        - Improve cloud computing capability
        - Modernize the network
        - Increase infrastructure efficiency
    - Improve communication and collaboration capabilities
        - Develop a unified communications strategy
        - Fully implement and leverage office 365
        - Develop a content management strategy
    - Manage IT risks and access
        - Modernize identity and access management
        - Conduct end user threat training
        - Enable network assurance

## TX, 2016-2020 State Strategic Plan for Information Resources Management (2 Goals, 6 Objectives)

- Secure and protect government and citizen information
  - Implement policies and standards aligned with the state's cybersecurity framework
  - Develop and adhere to a software currency policy
  - Increase employee cybersecurity training and awareness
- Prepare for continued government operations during and after an emergency
  - Test and improve business COOP
  - Consider cloud infrastructure to improve business continuity
  - Implement teleworking to improve COOP

## VA, Strategic Plan for IT, 2012-2018 (1 Goal, 6 Strategies)

- Implement technologies, practices, and monitoring to protect commonwealth data and infrastructure, reduce the commonwealth's attack surface area, maintain cyber security situational awareness, effectively respond to cyber security attacks, identify and remediate IT security risks, maintain a knowledgeable cyber security workforce, and maintain citizen trust in the commonwealth's commitment to the securing of their personal information.
  - Manage the IT risk management program for the commonwealth, including implementation of a risk management portfolio tool
  - Enhance the commonwealth's cyber security posture
  - Continue to enhance the cyber security governance framework to include:
    - Implementation of a method framework to ensure compliance with security PSGs,
    - Monitoring of commonwealth data and assets for threats and vulnerabilities and remediation of any issues identified,
    - Identification, mitigation, and management of IT security incidents,
    - Development of cyber intelligence based on research of current cyber trends as well as analysis of cyber data within the commonwealth, and
    - Provision of cyber security data and information to commonwealth entities and other partners of the commonwealth.
  - Develop security governance requirements for commonwealth identity management
  - Deploy a single identity management system (CAS) for all public-facing state government apps
  - Provide adequate cyber security training and education for commonwealth leaders, IT professionals, information security personnel, and commonwealth employees

## VT, 5 Year Strategic Plan FY2016-2020 (1 Goal, 4 Objectives)

- Enhance information security
  - Manage data commensurate with risk
  - Maintain defense in depth
  - Provide enhanced security awareness

## WV, Information Cyber Security Strategic Plan (2015) (15 Goals, 65 Policy Initiatives)

- Security Policy Development
  - Periodically update the existing executive branch security policies and procedures
  - Create additional policies and procedures as needed
  - Review agency information/cyber security policies
  - Maintain copies of all adopted policies online for web access

    - Develop an effective awareness training strategy for policies, and implement this strategy
    - Maintain policies that address the expectations held for employees with critical technical roles
- Privacy Partnership
    - Provide security expertise to the privacy management team and state privacy officer and staff
    - Collaborate with the chief privacy officer on security and privacy concerns
    - Collaborate with the privacy office to achieve compliance with privacy mandates, laws, and best practices
- Risk Management
    - Review and update documentation of system characterizations
    - Identify existing relevant threats and vulnerabilities
    - Document existing controls in place, or available, to reduce risk
    - Determine likelihood and impact of adverse event
    - Create a qualitative risk matrix: high, medium, and low
    - Conduct a cost-benefit analysis on prospective risk reduction options
    - Select a risk mitigation strategy based upon risk, cost-benefit analysis, and available resources
    - Recommend changes in controls/countermeasures. Work toward selection and commitment
    - Complete selected mitigation activities.
    - Create risk memoranda to identify residual/acceptable risk after controls/countermeasures
    - Monitor system for changes and repeat process at appropriate intervals
- Business Continuity Plan
    - Support activity of agency data and system classification
    - Support/validate meaningful alignment between business continuity and disaster recovery plans
    - Support/require periodic testing of business continuity plans, in conjunction with the associated disaster recovery plan
- Disaster Recovery Plans
    - Where agency agreements exist, verify that disaster recovery plans are completed for each critical business function, and aligned with the associated business continuity plan
    - Where agency agreements exist, verify that the plan for adequate periodic testing and validation of disaster recovery plans is completed and documented
- Security Operations Center
    - Maintain the full functionality needed in the SOC
    - Maintain 24x7x365 security surveillance of network traffic and system events for all critical infrastructure components combining threat analysis and alerts to State technicians when any anomalies are detected, correlated
    - Maintain comprehensive WEB activity monitoring and selective site blocking based upon customer requirements
    - Develop a state-of-the art situational watch room, combining analyst, management, and executive-level dashboards
    - Focus upon the insider threat, and network violation management through the use of effective policy monitoring, reporting and agency enforcement
    - Maintain and support the analysis of cyber-security counter-intelligence
- Training and Culture

    - Provide all executive branch employees with security awareness training, annually
    - Establish a process to audit for, and assure, completion of training by all employees, with proper documentation of training history
    - Establish minimum training standards, and assist with curriculum development that addresses the unique and/or elevated responsibilities and requirement for expertise, commensurate with the role
    - Offer WEB-based information/cyber security awareness training to local governments and other State partners
    - Conduct an annual "October is Cyber and Information/Cyber Security Awareness Month" event
    - Periodically introduce new or enhanced training to keep the message "fresh and effective."
- Information/Cyber Security Management Emphasis
    - Maintain an informed and engaged GEIST through quarterly meetings, ad hoc communications, information/cyber advisories, and special meetings, as needed
    - Elevate the visibility of the information security initiatives and the GEIST in organizational units throughout the state government
    - Periodically review the GEIST Charter for relevance and suitability
- Audit Program
    - Conduct audits in agencies for compliance with executive branch IT policy
    - Conduct audits of technical environments, with emphasis on the WVOT, for compliance with policy and best practices
    - Formal reporting of findings to appropriate management with recommendation for corrective action to mitigate identified risk
    - Conduct vulnerability scans, and oversee penetration testing as needed to verify system "health."
    - Contract for 3rd party auditing services to augment internal audit resources or to perform specialized audit services.
    - Review 3rd party provider agreements and services, including at off-site locations, to ensure adequate security controls
- Certification and Accreditation (C&A)
    - Identify responsibility and resources for the development of a C&A program
    - Establish the framework (processes, practices, and procedures) for C&A, collaborating within the office of technology, and between the WVOT and its State agency partners
    - Define C&A criteria and scope, meaning: what kinds of technologies must undergo C&A before being moved into production, and what are the standards that must be met for each technology
    - Plan, develop and deliver C&A training to all affected individuals, to unify understanding of the process, and understanding about how to approach product and service rollouts within the C&A framework.
    - Map C&A activities to the technology, and project-management life-cycle
- Incident Management and Computer Forensics
    - Maintain a computer security incident response team (CSIRT)
    - Maintain adequate forensics skills to accomplish needed investigations
- Staffing Levels and Team Development
    - Maintain a job classification series that closely describes required expertise, and the work, of an information/cyber security professional
    - Train and cross-train staff to a multi-disciplinary model as much as possible.
- Funding

    - Establish an adequate per seat per user fee for security services that will fund a fully functional information/cyber security controls and compliance program as described in this document
- Information/Cyber Security Metrics
    - Work with a representation of partners to develop a set of metrics to be identified and tracked
    - Determine how to derive the metric, and most efficiently capture and report the metric at the specified interval
    - Automate the metrics reporting function wherever possible
    - Continue to evaluate the effectiveness of the metrics strategy
- Outreach
    - Share expertise, assistance, and training materials with other public sector organizations
    - Promote discussions that will enhance the security work of all public sector partners in state government
    - Maintain active participation with the Multi State – Information Sharing Analysis Center and other groups whose reach is beyond the governor's executive branch
    - Maintain active participation in the National Association of State CIOs (NASCIO) Privacy and Security workgroup, and other relevant organizations
    - Maintain a working relationship with legislative commission on special investigations

**WI, Statewide Strategic IT Plan, 2014 (2 Goals, 4 Objectives)**

- Optimize Infrastructure and secure information with a focus on:
    - Security; and
    - Disaster Recovery/COOP

**WI Cyber Disruption Response Strategy, 2015 (5 goals, 20 objective's) (Not Publicly Available)**