GOALS & OBJECTIVES

GOAL 1 - SERVING WISCONSIN

Embrace self-service and digital-first service delivery through modern technology.

GOAL 2 - SECURING WISCONSIN

Secure State systems and data by refining strategies to mitigate risk for individuals and other key stakeholders, including operational changes due to unexpected events.

GOAL 3 - OPTIMIZING WISCONSIN

Modernize State agency legacy data and technology assets to achieve greater efficiency and effectiveness in delivering government services and operations.

GOAL 4 - WORKING WISCONSIN

Adopt practices that strengthen Wisconsin's State government workforce.

GOAL 2 - SECURING WISCONSIN

SECURE STATE SYSTEMS AND DATA BY REFINING STRATEGIES TO MITIGATE RISK FOR INDIVIDUALS AND OTHER KEY STAKEHOLDERS, INCLUDING OPERATIONAL CHANGES DUE TO UNEXPECTED EVENTS.

The State of Wisconsin has developed a "whole of state" approach program to provide leadership, share information, and develop resources for cybersecurity and its impact on the citizens, industry, infrastructure and government of the State of Wisconsin. Wisconsin's "whole of state" approach has been a point of discussion for the National Governors Association (NGA), a organization of the nation's governors that share best practices and speak with a collective voice on national policy. As part of the State's ongoing focus, efforts will continue to address appropriate protection, response, education, compliance, engagement, and transformation practices to secure State systems and data while mitigating risk.

- ***OBJECTIVE 1: Pursue statewide efforts to strengthen cybersecurity and enhance risk mitigation practices.***
- ***OBJECTIVE 2: Expand the State's cyber incident response capabilities.***
- ***OBJECTIVE 3: Improve Zero Trust and Application Security.***
- ***OBJECTIVE 4: Enhance education, information sharing and relationship building amongst cyber professionals and stakeholders statewide.***

OBJECTIVE 1: PURSUE STATEWIDE EFFORTS TO STRENGTHEN CYBERSECURITY AND ENHANCE RISK MITIGATION PRACTICES.

The State of Wisconsin is moving aggressively to strengthen its cybersecurity practices based on the National Institute of Standards and Technology (NIST) Cybersecurity framework. The Division of Enterprise Technology is leading with an enterprise approach, implementing advanced firewalls, a state-of-the-art Security Information and Event Management tool, and advanced cybersecurity hunting and response. The State is also actively partnering with other agencies and other entities at the State data center to maintain the security of all State data and systems. With the latest updates to NIST's cybersecurity framework, DET has added new controls for supply chain risk management and personally identifiable information processing and transparency.

Enterprise focuses over the coming biennium include:

- Ensuring that cybersecurity threats are mitigated through the correct combination of people, processes, and technology,
- Focusing on collaboration – cybersecurity is a team sport,
- Building security into processes and systems from the beginning,
- Establishing a culture of information sharing with government and private-sector partners to supplement and strengthen our defenses,
- Creating opportunities to teach and train cybersecurity, rather than simply quoting regulations and requirements, and
- Establishing a MyWisconsin ID for residents to securely access government services and systems.

Many states are also enacting laws to strengthen privacy protections for state residents using the internet. We are currently examining how we can strengthen privacy protections for people in Wisconsin.

OBJECTIVE 2: EXPAND THE STATE'S CYBER INCIDENT RESPONSE CAPABILITIES.

The State of Wisconsin established a volunteer cyber incident response team to respond to significant cyber incidents occurring within the State of Wisconsin. The cyber response team also assists State and local government agencies with preventative measures like penetration testing and other cybersecurity measures to identify and fix cybersecurity issues.

DET is focused on formally adopting clear roles, responsibilities, and capabilities for the cyber response team, developing a catalog of capabilities to provide greater awareness for partners throughout the State, and establishing a process between cyber incident response and physical consequence management.

DET is leading a joint effort with the Department of Public Instruction, University of Wisconsin System (UW System), and local school districts to include cybersecurity coursework in educational curricula to encourage students to consider cybersecurity careers to increase our resource capabilities within the State. DET is also working with the UW System to provide cybersecurity technology classes through the UW System's continuing education division, allowing anyone in the state of Wisconsin to take critical classes at a low cost. These technology classes will help bolster our State technical capabilities in preparing for and responding to cyber events.

OBJECTIVE 3: IMPROVE ZERO TRUST AND APPLICATION SECURITY.

As with many public and private organizations, the State of Wisconsin is currently transitioning to a mature zero trust model that incorporates best practices. In January 2022[5], the federal Office of Management and Budget announced that the federal government is formally moving towards a zero-trust architecture. Integral to this model are alignment with the five pillars identified by the Cybersecurity and Infrastructure Security Agency, including: Identity, Devices, Networks, Applications and Workloads, and Data.

This model will protect all layers of the digital estate by explicitly and continuously verifying each transaction, applying the principle of least privilege, and relies on intelligence, advanced detection, and real-time response to threats. This acknowledges the maturity of each agency and provides flexibility and agility in implementation.

Through the adoption of a zero-trust model, protections will be as close as possible to the data and systems being protected. Agencies can no longer rely on network perimeter protection to guard applications from unauthorized access.

The State will use ongoing monitoring and validation to allow authenticated users to access systems while flagging potential misuse. The principle of least privilege will restrict users to only those resources needed to complete their tasks and limits permissions. Additional identity security enhancements, like multi-factor authentication, will continue to reduce the ability of bad actors to access State systems. Combined with our enhanced application security efforts, these changes will greatly increase the security of our systems.

OBJECTIVE 4: ENHANCE EDUCATION, INFORMATION SHARING AND RELATIONSHIP BUILDING AMONGST CYBER PROFESSIONALS AND STAKEHOLDERS STATEWIDE.

The federal government[6] has made information sharing a key priority over the next several years, including the maturation and expansion of the national fusion center network to share information on cybersecurity threats. Specifically, the Cybersecurity and Infrastructure Security Agency has developed numerous methods to permit the safe sharing of sensitive cybersecurity information.

Most importantly, the State is emphasizing collaboration among cyber professionals, stakeholders, and other partners. This includes the development of a mechanism to share intelligence and information, continued hosting of the Governor's Conference on Cybersecurity, and identifying new sectors and industries where partnerships can increase cybersecurity.