NASEO State Energy Cybersecurity Models Analysis: Michigan Cybersecurity Structures and Programs Profile

NASEO State Energy Cybersecurity Models Analysis:

Michigan Cybersecurity Structures and Programs Profile

Prepared by
National Association of State Energy Officials
2107 Wilson Boulevard, Suite 850
Arlington, Virginia 22201
Telephone: 703.299.8800
Website: www.naseo.org

December 2015

National Association of
State Energy Officials

Disclaimer of Warranties and Limitation of Liabilities

Acknowledgment of work by the National Association of State Energy Officials contributing to this effort:

This material is based upon work supported by U.S. Department of Energy under award DE-OE0000583.

Disclaimer:
This report was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or any agency thereof.

THE FOLLOWING ORGANIZATION PREPARED THIS REPORT:
National Association of State Energy Officials
2107 Wilson Boulevard, Suite 850 Arlington, Virginia 22201-3091
Telephone: 703.299.8800; Fax: 703.299.6208
Website: www.naseo.org

The National Association of State Energy Officials

The National Association of State Energy Officials (NASEO) is the only national non-profit organization whose membership includes governor-designated energy officials from each of the 56 states and territories. Formed in 1986, NASEO facilitates peer information exchange among state energy officials, serves as a resource for and about State Energy Offices, and advocates the interests of the State Energy Offices to Congress and federal agencies.

Members are senior officials from State and Territory Energy Offices, as well as affiliates from the private and public sectors. Member State Energy Offices work on a wide range of energy programs and policies, including those which shape:

- Energy efficiency in all market sectors, including buildings, industry, and agriculture;
- Renewable energy, such as solar, wind, geothermal, and biomass;
- Advanced transportation technologies, alternative fuels and infrastructure;
- The production and distribution of oil, natural gas, and electricity;
- Energy-environment integration and the promotion of cost-effective energy solutions; and
- Energy system resiliency, Energy Assurance, cybersecurity, and supply disruption preparedness and response.

States manage and invest more than $8 billion of their own funds each year. These funds are derived from state appropriations, system benefit charges, and other nonfederal sources and are utilized to advance cost-effective energy efficiency actions that aid consumers and businesses in reducing energy costs while enhancing economic competitiveness.

Table of Contents

Acknowledgements

The National Association of State Energy Officials (NASEO) prepared this document to promote peer information exchange between states by identifying and profiling Michigan's innovative statewide cybersecurity structure and programs.

The primary authors of this report include Jeffrey Pillon and Shemika Spencer of NASEO. NASEO is grateful for the review and input from personnel within the following state agencies: Michigan Department of Technology, Management, and Budget; Michigan State Police; Michigan Department of Licensing and Regulatory Affairs; Michigan Agency for Energy, Michigan Public Service Commission; and Michigan Department of Military and Veteran Affairs.

Introduction

Over the last 15 years there has been a significant increase in the number and sophistication of cyber-attacks which threaten this nation's economy, infrastructure, security, and way of life. In February 2013, President Obama issued the *Executive Order on Improving Critical Infrastructure Cybersecurity* (EO 13636)[1] and the *Presidential Policy Directive on Critical Infrastructure Security and Resilience* (PPD – 21)[2] which recognize the vulnerabilities of our power, water, communication, and other critical systems against cyber-attacks and the need for holistic thinking about security and risk management.

EO 13636 is designed to increase the nation's capacity to manage the cyber risk facing our critical infrastructure. It does this by focusing on three key areas: (1) information sharing, (2) privacy, and (3) the adoption of cybersecurity practices. In addition, EO 13636 tasked the National Institute for Standards and Technology (NIST) to work with the private sector to identify existing voluntary consensus standards and industry best practices and build them into a Cybersecurity Framework, and it directed the U.S. Department of Homeland Security (DHS) to establish a voluntary program to promote the adoption of the Framework. Furthermore, EO 13636 called for federal agencies, as well as state and local governments, to evaluate how they will use the Framework to enhance the protection of their systems and leverage capabilities found in the Framework to assist in managing their cybersecurity risk.

PPD – 21, which replaced a prior directive, calls for the Executive Branch to strengthen critical infrastructure security and resilience by: (1) developing a situational awareness capability, (2) understanding the cascading consequences of infrastructure failures, (3) evaluating and maturing the public-private partnership, (4) updating the National Infrastructure Protection Plan, and (5) developing a comprehensive research and development plan. As the Sector-Specific Agency for the energy sector, the U.S. Department of Energy (DOE) was directed to coordinate with the Electricity Sector Coordinating Council (Electric SSC) and the Oil and Natural Gas Sector Coordinating Council (ONG-SSC) to review the Framework and develop guidance and supplemental materials to address sector-specific risks and operating environments.

NASEO, in support of federal efforts to implement the President's directives outlined in EO 13636 and PPD – 21, and to assist states in meeting their own policy goals, provides State Energy Offices with information from their state peers on federal efforts to improve cybersecurity, encourages public-private collaborations with Electric SSC and ONG-SSC when appropriate, and encourages states to consider cybersecurity when updating their energy assurance plans.

For example, *NASEO's Energy Assurance Guidelines*[3] emphasize the need for state energy agencies (e.g., State Energy Offices and Public Utility Commissions) to recognize the

[1] Executive Office of the President. Executive Order on Improving Critical Infrastructure Cybersecurity (EO 13636). February 12, 2013. Accessed on February 10, 2015. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[2] Executive Office of the President. Presidential Policy Directive on Critical Infrastructure Security and Resilience. February 12, 2013. Accessed on February 10, 2015. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[3] National Association of State Energy Officials. State Energy Assurance Guidelines Version 3.1. December 2009. Accessed on February 10, 2015. http://www.naseo.org/Data/Sites/1/documents/energyassurance/eaguidelines/State_Energy_Assurance_Guidelines_Version_3.1.pdf

importance of cybersecurity and assign staff resources on an ongoing basis. In addition, the Guidelines recommend providing ongoing cybersecurity training for personnel to ensure a sufficient depth of knowledge as needed. Furthermore, in 2011, NASEO developed a whitepaper which discussed smart grid and cybersecurity issues in more detail which was entitled, *"Smart Grid and Cyber Security for Energy Assurance: Planning Elements for Consideration in States' Energy Assurance Plans"*.[4] The papers recommend the following five (5) step approach to building states' cybersecurity capabilities:

1) Understand the state's internal cybersecurity profile;
2) Understand the current cybersecurity requirements for the energy sector;
3) Understand future standards and guidelines currently under discussion and development and how they may affect utilities' plans for smart grid deployment;
4) Determine whether there are cybersecurity plans in place and whether they are driven by state regulatory or federal grants compliance; and
5) Consider and address the human element of cybersecurity.

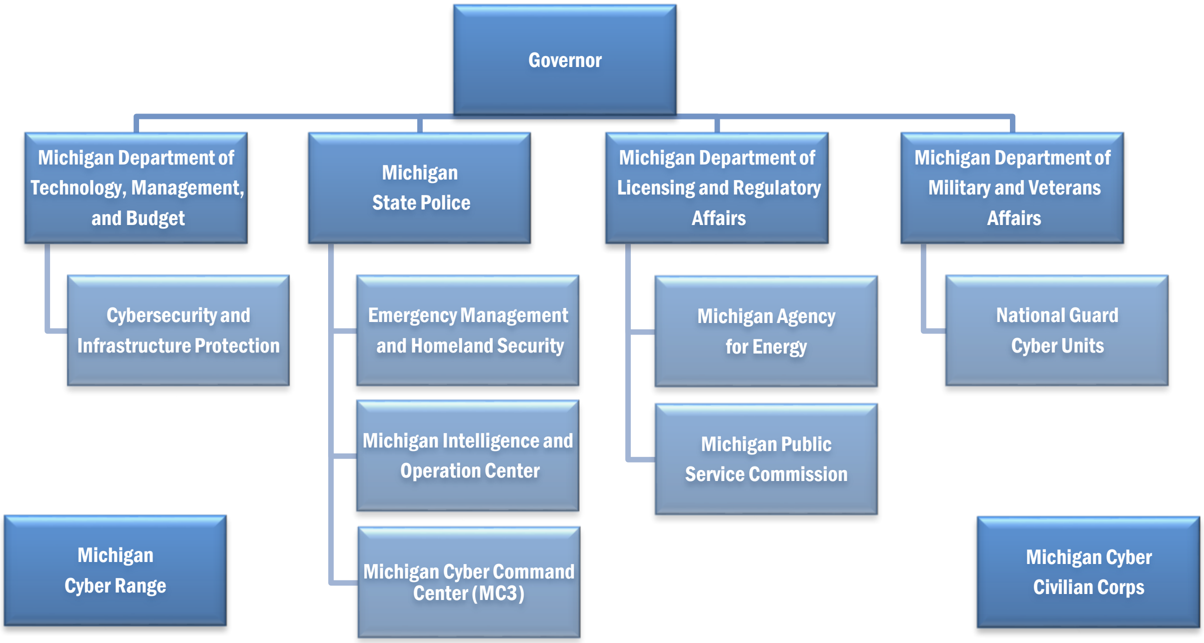
In support of states' efforts to develop and improve institutional cybersecurity capabilities, NASEO promotes peer information exchange among states by identifying and profiling states' innovative cybersecurity structure and programs. This analysis is the first of two reports which examines how specific states address cybersecurity through the implementation of statewide policies, regulations, and programs. This report profiles cybersecurity in Michigan and looks at how strong leadership from the governor, along with the involvement of key state agencies, guides the roles and responsibilities for cybersecurity. It also explores how cybersecurity is being addressed through public-private collaborations and identifies how Michigan is responding to the various federal efforts to improve cybersecurity.

[4] National Association of State Energy Officials. Smart Grid and Cyber Security for Energy Assurance: Planning Elements for Consideration in States' Energy Assurance Plans. Pages 16 – 22. November 2011. Accessed on February 10, 2015. http://www.naseo.org/data/sites/1/documents/publications/NASEO_Smart_Grid_and_Cyber_Security_for_Energy_Assurance_rev_November_2011.pdf

Roles and Responsibilities for Cybersecurity in the State of Michigan

Michigan has an established effort supporting overall cybersecurity which includes strong leadership from the Governor and working collaboratively with the energy sector. The information in this report was compiled from publically available information and from a series of meetings with relevant Michigan state agencies involved in cybersecurity activities. In addition, a draft of this report was shared with the agencies assisting with this effort to clarify and ensure that all key initiatives and programs were included and properly described.

The roles and responsibilities of the following key state agencies were examined as part of this effort and each is described in further detail. Much of the information contained in this section has been taken verbatim from state agency websites or other publically available published information.


Governor
Michigan Department of Technology, Management, and Budget
Michigan State Police
Michigan Department of Licensing and Regulatory Affairs
Michigan Department of Military and Veterans Affairs
Cybersecurity and Infrastructure Protection
Emergency Management and Homeland Security
Michigan Intelligence and Operation Center
Michigan Cyber Command Center (MC3)
Michigan Agency for Energy
Michigan Public Service Commission
National Guard Cyber Units
Michigan Cyber Range
Michigan Cyber Civilian Corps

Michigan Governor's Leadership

Cybersecurity efforts in Michigan state government have been underway for many years. These efforts include strategies to address *Presidential Policy Directive – Critical Infrastructure Protection (PDD-63)*[5] issued on May 22, 1998, by President Clinton. Beginning in the late 1990s efforts were undertaken to assure that the state's information technology (IT) systems were prepared to deal with the year 2000 changeover (more commonly referred to as Y2K), and following 9/11 cybersecurity became a key component

[5] U.S. Government Printing Office. Presidential Policy Directive – Critical Infrastructure Protection (PDD – 63). May 22, 1998. Accessed on November 17, 2014. http://www.gpo.gov/fdsys/granule/FR-1998-08-05/98-20865.

of the state's critical infrastructure protection efforts. It has been estimated the U.S. spent in excess of $100 billion to address the Y2K problem in advance of 2000[6].

When Governor Snyder was elected in 2010, he brought with him a clear understanding of the importance of cybersecurity given his former role as president of Gateway Computers. Governor Snyder also had a personal experience with identity theft that only served to further deepen his understanding of the importance of cybersecurity.

In 2011, Governor Snyder launched the *Michigan Cyber Initiative* and issued an accompanying report, *Defense and Development for Michigan Citizens Businesses and Industry*[7]. This report opens with the following letter from the Governor that has set the tone for the work that has been underway since.

Letter from the Governor

The Internet's impact on our world continues to be profound. Whether we're chatting with friends, accessing government services or conducting global commerce, opportunities abound to enhance our daily lives through the convenience and speed afforded by technology.

Unfortunately, the Internet also provides new avenues for crime, misconduct and espionage. Last year alone, 8 million people reported cases of identity theft. More than $1 trillion in commerce has been lost and terabytes of data have been stolen or compromised.

In an equally disturbing trend, these crimes are now the province of professionals. Amateur "hacking" has given way to organized, sophisticated attacks on our personal safety and economic security.

Against that backdrop, Michigan is taking a leadership role in cyber defense and development for Michigan's citizens, businesses and industry. The Michigan Cyber Initiative is focused on protecting the vulnerable ecosystem in the cyber world.

This report underscores Michigan's commitment to cybersecurity. It is an action plan that offers clear approaches for safeguarding our families, protecting Michigan's infrastructure and shielding our economy. In keeping with Michigan's innovative spirit, these pages also outline ways in which our state will seize the economic opportunities spawned by the burgeoning field of cybersecurity.

Technology is Michigan's future. Our already heavy reliance on the Internet will only grow, making it imperative that we treat the issue of cybersecurity with the urgency it deserves.

I'm proud that once again, Michigan is taking a visionary, proactive approach to meeting its challenges and embracing opportunities. By working together, our state will be a national model of innovation, success and security.

Rick Snyder
Governor, State of Michigan

[6] Encyclopedia Britannica. Y2K bug. Accessed on November 17, 2014. http://www.britannica.com/EBchecked/topic/382740/Y2K-bug

[7] Michigan Executive Office of the Governor. Michigan Cyber Initiative – Defense and Development for Michigan Citizens Businesses and Industry. Accessed on November 17, 2014. http://www.michigan.gov/documents/cybersecurity/MichiganCyberInitiative2011_365631_7.pdf

The importance of executive leadership cannot be understated in ensuring that appropriate measures are taken in a coordinated fashion across state government. This initiative described its vision as follows:

> Michigan's vision is to secure this ecosystem and to continue its leadership in this domain. The *Michigan Cyber Initiative* is built around three distinct but equally important pillars:
>
> - **Confidentiality** (ensuring private information in the ecosystem remains private)
> - **Integrity** (ensuring that the information in the ecosystem is complete, whole and defensibly sound)
> - **Availability** (ensuring that the information in the ecosystem continues to be available to serve its purpose)

The vision further describes Michigan's cyber threat response, the importance of education and public awareness, collaboration and partnerships, and outlines a cybersecurity economic development strategy.

To track progress toward achieving the goals of the cyber initiative, Governor Snyder established a cybersecurity dashboard[8] designed to provide a regularly updated view of Michigan's cybersecurity environment.

At the national level, Governor Snyder, along with former-Maryland Governor Martin O'Malley, co-chaired the National Governors Association (NGA) Resource Center for State Cybersecurity. As a result of their efforts, the NGA released a paper in September 2013 entitled, "*Act and Adjust: A Call to Action for Governors for Cybersecurity"*[9], which calls for immediate actions to protect states which includes the following:

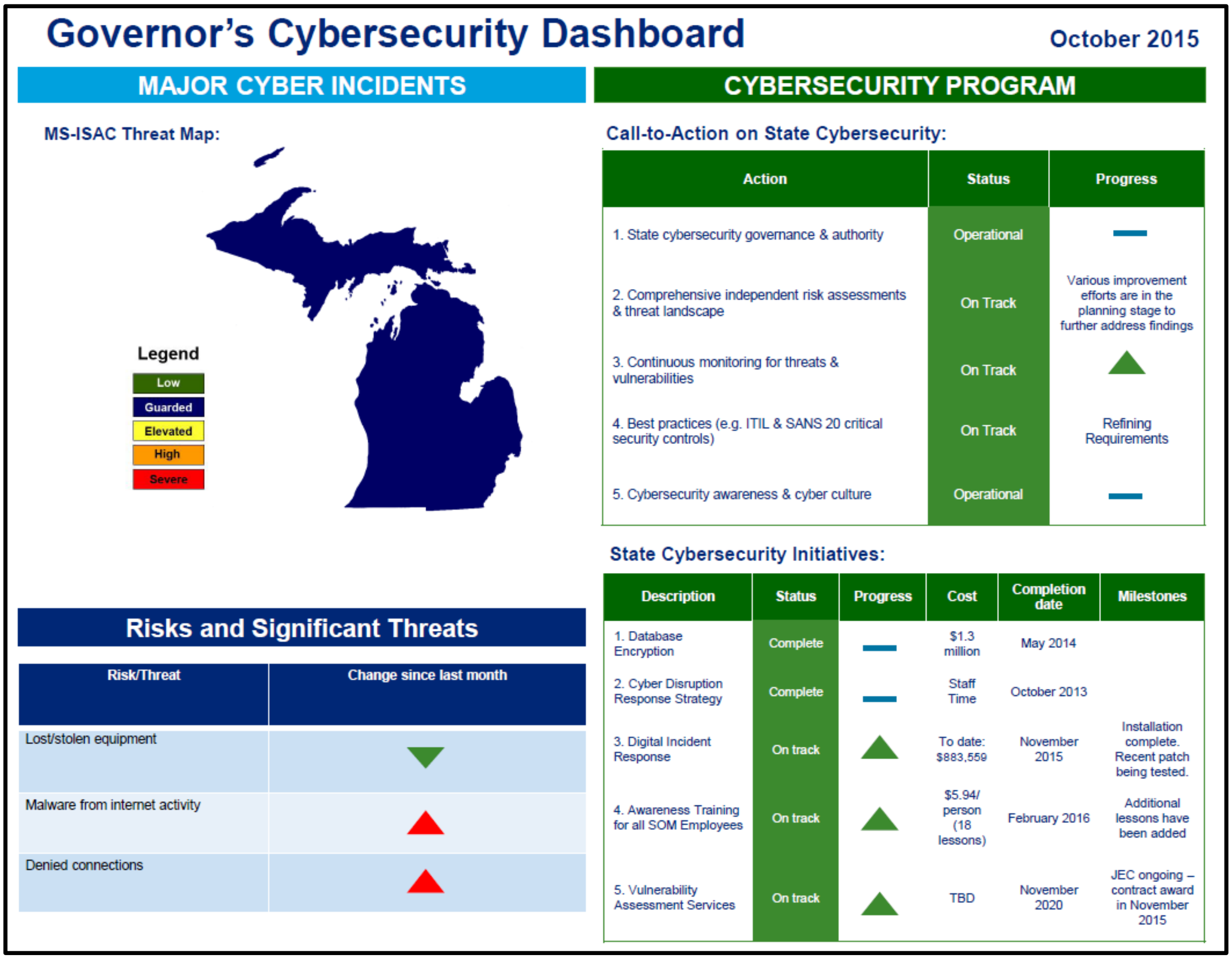
- Establish a governance structure for cybersecurity.
- Conduct risk assessments and allocate resources accordingly.
- Implement continuous vulnerability assessments and threat mitigation practices.
- Ensure compliance with current security methodologies and business disciplines in cybersecurity.
- Create a culture of risk awareness.

With the Governor's leadership, Michigan has also created a centralized security department run by a Chief Security Officer (CSO) that brings together both physical and cybersecurity personnel. Directors, managers, and employees within each agency coordinate through this centralized governance structure to address each agency's security needs. This governance structure provides a definitive hierarchy which simplifies communication channels in the event of an incident or a disaster. The approach allows the CSO and Chief Information

[8] Michigan Executive Office of the Governor. Governor's Cybersecurity Dashboard, October 2015. http://www.michigan.gov/documents/cybersecurity/Governors_Cybersecurity_Dashboard_OCT_2015p_505215_7.pdf

[9] National Governors Association's Resource Center on Cybersecurity. Act and Adjust: A Call to Action for Governors for Cybersecurity. September 2013. Accessed on November 17, 2014. http://www.nga.org/files/live/sites/NGA/files/pdf/2013/1309_Act_and_Adjust_Paper.pdf

Officer to work closely to manage the state's cyber networks and infrastructure and to ensure that effective governance practices are in place.



Governor's Cybersecurity Dashboard

October 2015

MAJOR CYBER INCIDENTS

MS-ISAC Threat Map:

Risks and Significant Threats

Risk/Threat	Change since last month
Lost/stolen equipment	▼
Malware from internet activity	▲
Denied connections	▲

CYBERSECURITY PROGRAM

Call-to-Action on State Cybersecurity:

Action	Status	Progress
1. State cybersecurity governance & authority	Operational	—
2. Comprehensive independent risk assessments & threat landscape	On Track	Various improvement efforts are in the planning stage to further address findings
3. Continuous monitoring for threats & vulnerabilities	On Track	▲
4. Best practices (e.g. ITIL & SANS 20 critical security controls)	On Track	Refining Requirements
5. Cybersecurity awareness & cyber culture	Operational	—

State Cybersecurity Initiatives:

Description	Status	Progress	Cost	Completion date	Milestones
1. Database Encryption	Complete	—	$1.3 million	May 2014	
2. Cyber Disruption Response Strategy	Complete	—	Staff Time	October 2013	
3. Digital Incident Response	On track	▲	To date: $883,559	November 2015	Installation complete. Recent patch being tested.
4. Awareness Training for all SOM Employees	On track	▲	$5.94/ person (18 lessons)	February 2016	Additional lessons have been added
5. Vulnerability Assessment Services	On track	▲	TBD	November 2020	JEC ongoing – contract award in November 2015

The Governor has also sponsored four Cybersecurity Summits, held in 2011, 2013, 2014, and 2015, that brought together the public and private sector to forge a better understanding of the cybersecurity risks and actions needed to help reduce cyber-attacks.

The 2011 summit -- purposely held during National Cyber Awareness Month -- was used to introduce the *Michigan Cyber Initiative* and to articulate a shared vision for Michigan's cyber future. . The following Summit, held in 2013, was highlighted by the announcement of the formation of the Michigan Cyber Civilian Corps, a first-of-its-kind cadre of volunteer IT experts who are trained to assist in the event of a major cyber-attack to Michigan's critical infrastructure.

The third Summit announced the *Michigan Cyber Initiative 2015*[10] which chronicles the state's cybersecurity accomplishments since 2011 and those expected to take place over the next four years. The document outlines initiatives in the following key areas:

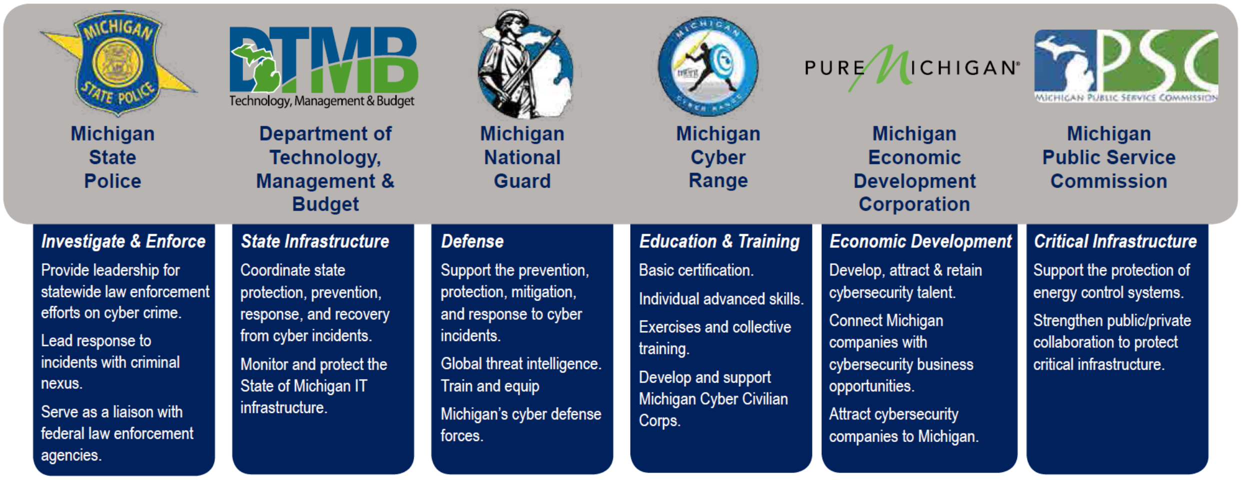
[10] Michigan Executive Office of the Governor. Michigan Cyber Initiative 2015. November 2014. Accessed on December 1, 2014. http://mi.gov/documents/cybersecurity/Mich_Cyber_Initiative_11.13_2PM_web_474127_7.pdf

- Leadership, Prevention, Detection, Response
- Education and Public Awareness
- Michigan’s unique cyber industry opportunity
- Michigan’s Cybersecurity Ecosystem

Notable in the *Michigan Cyber Initiative 2015* is the recognition of the importance of the energy sector and the efforts of the Michigan Public Service Commission to address cybersecurity.

The 2015 Summit[11] stressed the importance of improved coordination and sustained vigilance as Michigan continues into an era of increased dependence on information technology. In his keynote address, Governor Snyder noted that the State of Michigan now fends off over 2.5 million cyber-attacks per day, and that meeting such a growing challenge will require a state-wide effort to train and retain top cyber professionals.

The following figure from the *Michigan Cyber Initiative 2015* show the roles of the various state agencies involved in cybersecurity which are described in further detail in the balance of this report.


MICHIGAN STATE POLICE
DTMB
Technology, Management & Budget
MICHIGAN CYBER RANGE
PURE MICHIGAN
PSC
MICHIGAN PUBLIC SERVICE COMMISSION

Michigan State Police

Investigate & Enforce

Provide leadership for statewide law enforcement efforts on cyber crime.

Lead response to incidents with criminal nexus.

Serve as a liaison with federal law enforcement agencies.

Department of Technology, Management & Budget

State Infrastructure

Coordinate state protection, prevention, response, and recovery from cyber incidents.

Monitor and protect the State of Michigan IT infrastructure.

Michigan National Guard

Defense

Support the prevention, protection, mitigation, and response to cyber incidents.

Global threat intelligence. Train and equip

Michigan's cyber defense forces.

Michigan Cyber Range

Education & Training

Basic certification.

Individual advanced skills.

Exercises and collective training.

Develop and support Michigan Cyber Civilian Corps.

Michigan Economic Development Corporation

Economic Development

Develop, attract & retain cybersecurity talent.

Connect Michigan companies with cybersecurity business opportunities.

Attract cybersecurity companies to Michigan.

Michigan Public Service Commission

Critical Infrastructure

Support the protection of energy control systems.

Strengthen public/private collaboration to protect critical infrastructure.

Michigan Cyber Range/Merit Network, Inc.

Merit Network, Inc. is a nonprofit, member-owned organization formed in 1966 to design and implement a computer network between public universities in Michigan. Merit continues to leverage its experience managing the National Science Foundation Network or NSFNET, a precursor to the modern internet, to enhance Michigan’s infrastructure for networking technologies. Merit maintains a 10 gigabit per second backbone which it has since extended across the state to continue to provide a flexible, robust architecture to support research and education needs. This enhanced capacity is completely self-funded.

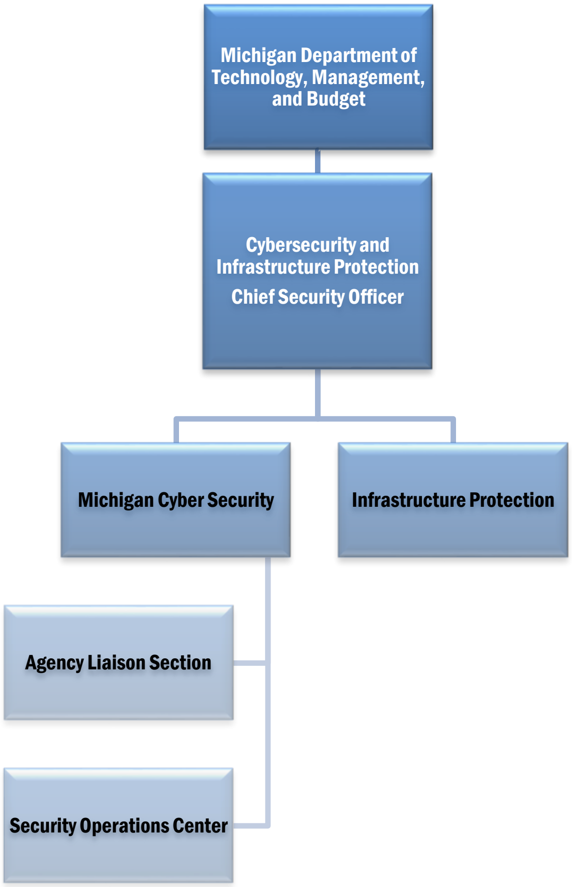
[11] 2015 North American International Cyber Summit, October 25-26, 2015http://events.esd.org/CyberSummit.aspx

The Michigan Cyber Range[12], which opened in November 2012, was developed as a response to the Governor's cyber initiatives. It is hosted by Merit Network, Inc. in Ann Arbor, Michigan and operates as a public-private sector collaboration between government, the National Guard, universities, community colleges, K-12 schools, and the private sector. The Cyber Range enables individuals and organizations to develop detection and reaction skills through simulations and exercises. It provides a unique testing environment that allows large- and small-scale networks to be simulated using a mixture of virtual and physical devices. Once a network has been placed onto the Cyber Range it can be attacked and defended without having to place the organization's actual networks at risk. The program offers students and IT professionals a full curriculum of meetings and workshops as well as critical cybersecurity training and awareness tools. In March 2014, the Michigan National Guard connected its first Cyber Range Hub to the Michigan Cyber Range at the 110th Air Wing in Battle Creek. This was quickly followed by Camp Grayling, the largest Army National Guard Training Center in the country, and by Fort Custer in Battle Creek. There are plans to connect additional Michigan installations as well as to partner with National Guard installations across the country.

Michigan Cyber Range partners include Merit Network, Inc., DHS, DOE, National Institute of Standards and Technology, DTE Energy, Consumers Energy, Plante and Moran PLLC, Juniper Networks, Eastern Michigan University, Michigan State Police, Michigan Department of Military and Veterans Affairs, Michigan Economic Development Corporation, and the Michigan Department of Technology, Management, and Budget.

Michigan Department of Technology, Management, and Budget's Office of Cybersecurity and Infrastructure Protection

Housed within the Michigan Department of Technology, Management, and Budget (DTMB) is the Office of Cybersecurity and Infrastructure Protection, which is the single entity charged by Governor Snyder with the risk management and operational oversight of physical and cybersecurity missions associated with government assets, data, property, systems, and networks. It is headed by the CSO and is organized as shown at right. Among the activities it supports are:


Michigan Department of Technology, Management, and Budget
Cybersecurity and Infrastructure Protection Chief Security Officer
Michigan Cyber Security
Infrastructure Protection
Agency Liaison Section
Security Operations Center

[12] Michigan Executive Office of the Governor, Governor Launces Cutting-Edge Cybersecurity Training Program. November 9, 2012. Accessed on November 18, 2014. http://www.michigan.gov/snyder/0,4668,7-277-57577-289758--,00.html

- The "Kitchen Cabinet," where public and private sector CSOs meet periodically to collaborate and share information and best practices
- The Cyber Civilian Corps, a rapid response team of cybersecurity experts
- Michigan Cyber Awareness Luncheons
- The Michigan Cyber Initiative newsletter
- Education and training for citizens, businesses, and government (90+% of state employees have had cybersecurity awareness training, which they rated highly)
- The Federal Bureau of Investigation's (FBI) InfraGard Program
- The Michigan Cybersecurity website, which provides extensive educational information and toolkits to promote cybersecurity for citizens, businesses, and government

The *Michigan Cyber Disruption Response Strategy* was prepared by the DTMB, the Michigan State Police, and the Michigan Department of Military and Veterans Affairs (DMVA). As stated in the document, the *Michigan Cyber Disruption Response* Strategy *"provides a framework to assist critical infrastructure owners and operators in the development of a collaborative, public/private team to respond to cyber disruption events affecting the State of Michigan. This strategy was developed by representatives from various critical infrastructure owners in Michigan, and state and local government officials. The overall intent of this framework is to limit the impact of cyber disruptions in the state, and thus maintain critical services for the public."*[13]

The strategy established goals and objectives which are dependent upon voluntary resources put forth by participating critical infrastructure owners and operators and government agencies. The CSO and DTMB are responsible for the overall administration and maintenance of this plan and the monitoring and reporting of its progress. These efforts will be coordinated with the Michigan State Police, which is ultimately responsible for statewide emergency management and homeland security as well as coordinating the protection of Michigan's critical infrastructure.

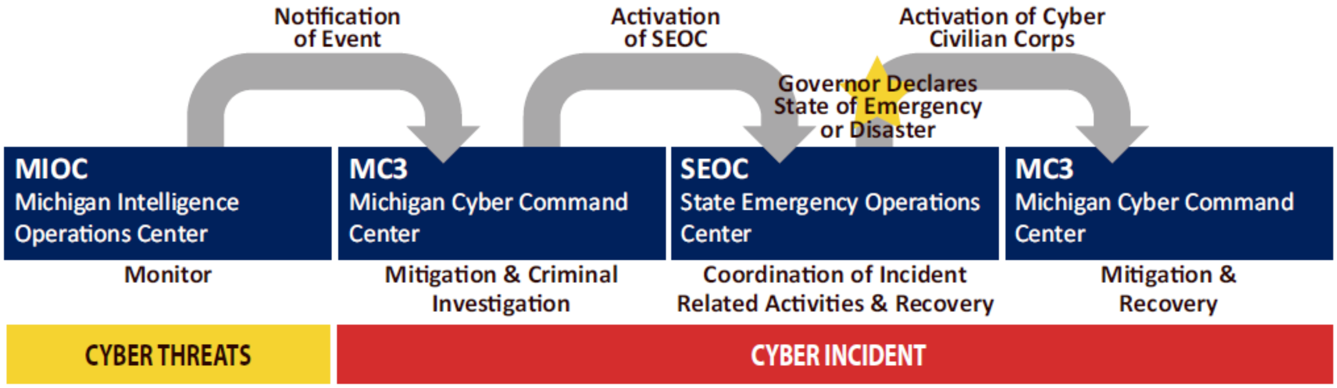
In October 2015, the DTMB, the MSP, and the DMVA released a follow-up document, the Michigan Cyber Disruption Response Plan[14] which builds off the *Strategy* and better allows the State of Michigan to keep pace with the evolving nature of the cyber threats.

As stated in the executive summary, *"This plan provides a common framework for identifying and responding to technological threats by defining five threat levels that mirror the federal government model, with corresponding responses to address threats of increasing scope and severity. These cyber disruption threats range from minor malware incidents; through specific attacks on targeted state networks and services; to severe attacks capable of catastrophic impact to services and facilities of single or multiple sectors providing critical support to citizens government, public and private entities. The plan enables closely integrated planning by providing a standard incident response plan template for critical infrastructure entities and partnership use."*

[13] Michigan Department of Technology, Management, and Budget, et al. Michigan Cyber Disruption Response Strategy. Page 1. September 16, 2013. Accessed on November 18, 2014. http://www.michigan.gov/documents/cybersecurity/Michigan_Cyber_Disruption_Response_Strategy_1.0_438703_7.pdf

[14] Michigan Department of Technology, Management, and Budget, et al. Michigan Cyber Disruption Response Plan, October 25, 2015. http://www.michigan.gov/documents/cybersecurity/102615_Michigan_Cyber_Disruption_Response_Plan_-_Reduced_504157_7.pdf

The process of prevention, detection, and response to cyber events is shown in the following figure found in the *Michigan Cyber Initiative 2015*[15].


Notification of Event
Activation of SEOC
Activation of Cyber Civilian Corps
Governor Declares State of Emergency or Disaster
MIOC
Michigan Intelligence Operations Center
MC3
Michigan Cyber Command Center
SEOC
State Emergency Operations Center
MC3
Michigan Cyber Command Center
Monitor
Mitigation & Criminal Investigation
Coordination of Incident Related Activities & Recovery
Mitigation & Recovery
CYBER THREATS
CYBER INCIDENT

The Michigan Cyber Civilian Corps (MiC3)[16] is a group of trained cyber experts who individually volunteer to provide expert assistance to the state in times of emergency. MiC3 provides rapid response to cyber incidents which prompt a governor declared state of emergency. MiC3 was created through a partnership with the DTMB, the Michigan State Police, the National Guard, and other public and private partners. The group includes volunteers from government, education, and business sectors. As of March 2015, the MiC3 has about 30 members and is actively recruiting volunteers to serve across the state's 10 regions. This will ensure that companies and government agencies in all parts of the state, but especially rural areas, have access to trained security professionals in the wake of a major incident.

Emergency Management and Homeland Security Division/Michigan State Police

The Emergency Management and Homeland Security Division (EMHSD), which is part of the Michigan State Police, is responsible for statewide emergency management and homeland security. The EMHSD Commander serves as the Deputy State Director of Emergency Management and Homeland Security and is responsible for the statewide management and administration of emergency management and homeland security programs. The Division also maintains the Michigan Emergency Management Plan, conducts training and exercises, and is responsible for the State Emergency Operations Center (SEOC) and its activation. Upon full activation, emergency management coordinators from each principal department of state government will report to the SEOC to assist in the emergency response effort.

EMHSD, in coordination with its partners, developed a *Statewide Homeland Security Strategy*[17] covering the period 2009 – 2013 which integrated the state's collective efforts to

[15] Michigan Executive Office of the Governor, Michigan Cyber Initiative 2015. Page 6. November 2014. Accessed on December 1, 2014. http://mi.gov/documents/cybersecurity/Mich_Cyber_Initiative_11.13_2PM_web_474127_7.pdf
[16] Michigan Cyber Civilian Corps. Accessed on November 18, 2014. http://www.micybercorps.org/
[17] Michigan State Police, et al. Homeland Security Strategy. Accessed on November 18, 2014. http://www.michigan.gov/documents/msp/Homeland_Security_Strat_FINAL_362552_7.pdf

ensure the health, safety, and welfare of Michigan citizens. The strategy helps direct federal funding to bolster Michigan's capabilities to prevent, detect, and respond to all hazards. Fundamental to the development of the strategy was the use of a bottom-up approach which started with Michigan's seven homeland security regions. This approach ensured a balanced level of preparedness and response capabilities by coordinating planning efforts, sharing resources, and leveraging mutual aid agreements across the individual regions.

In June 2012, the EMHSD prepared the *Michigan Hazard Analysis*[18] in coordination with the *Michigan Emergency Management Plan* and *Michigan Hazard Mitigation Plan*. The document serves as a foundation for the development of other state plans and provides a large array of information for local communities to use when conducting their own hazard analyses. It defines a cyber-attack as *"a new category of terrorist and criminal threat. Cyber-attacks involve the use of computers, electronic devices, and/or the Internet to attack computer systems"* and provides some examples of information that may be noted and reported about cyber-attacks.

Michigan Intelligence and Operation Center /Michigan State Police

The Michigan Intelligence Operations Center (MIOC)[19] – also known as the State fusion center – provides 24/7 statewide information sharing among local, state, and federal public safety agencies and private sector organizations in order to facilitate the collection, analysis, and dissemination of intelligence relevant to terrorism and public safety. Michigan's state fusion center includes active participation by federal, tribal, state, and local law enforcement partners along with the state's Department of Military and Veterans Affairs and the Department of Corrections. Additionally, the MIOC has established partnerships which allow other state agencies involved in homeland security initiatives to participate in fusion center activities. Partnerships are also being sought with various other private and public entities which are responsible for promoting public safety and protecting Michigan's critical infrastructure. The Michigan State Police is responsible for the MIOC's direction and management; however, all agencies participate in guiding the mission and operations of the center.

The private sector has an important role to play in the protection of our nation's critical infrastructure, as they desire to protect their assets, employees, and customers. Additionally, they are important sources of information, as private sector security teams often have better observational capabilities and a more intimate knowledge of the activities occurring around their facilities both locally and around the world. This data is often invaluable to a fusion center analyst attempting to identify emerging trends or threats.

The Critical Infrastructure Protection (CIP) Desk[20], which is located within the MIOC, is the centralized location for all critical infrastructure information, warnings, reporting, dissemination, and program coordination. The CIP Desk provides a critical interface between

[18] Michigan State Police. Michigan Hazard Analysis. Page 379. July 2012. Accessed on November 18, 2014. http://www.michigan.gov/documents/msp/Doc1_394216_7.pdf

[19] Michigan Intelligence Operations Center. Frequently Asked Questions. Accessed on November 18, 2014. www.michigan.gov/mioc/0,1607,7-241-44636---,00.html

[20] Michigan Intelligence Operations Center. Critical Infrastructure Protection (CIP) Desk. Accessed on November 18, 2014. http://www.michigan.gov/mioc/0,1607,7-241-55994---,00.html

the private and public sectors, and provides its partners with cyber-related threat information as needed. Roles and responsibilities of the CIP Desk include:

- Conducting public and private sector outreach to promote the capabilities of the MIOC.
- Maintaining and developing two-way communications between the desk and the Critical Infrastructure and Key Resources (CIKR) operators and security mangers to encourage cooperation in information sharing and management.
- Working with MIOC analysts to collect and vet suspicious activity reports.
- Serving as the state's link to DHS for CIKR programs and information sharing.
- Sharing information with private sector partners concerning cyber threats.

Michigan Cyber Command Center/Michigan State Police

The Michigan Cyber Command Center (MC3)[21] was created to coordinate the combined efforts of cyber emergency responders. The MC3 holds regular briefings, performs training, conducts exercises, and maintains dedicated resources to accommodate daily communication amongst state, local, and federal agencies as well as private sector business that participate with the MC3 or the MIOC. MC3 partners with, and has resources within, the FBI, DHS, United States Secret Service, United States Computer Emergency Readiness Team (US-CERT), DTMB, and others. Regular communication channels exist to provide state-wide visibility to current threats. The MC3 is the state's lead responder to incidents with a criminal nexus and is the state's resource for investigation, mitigation, and prosecution of cyber-crime incidents.

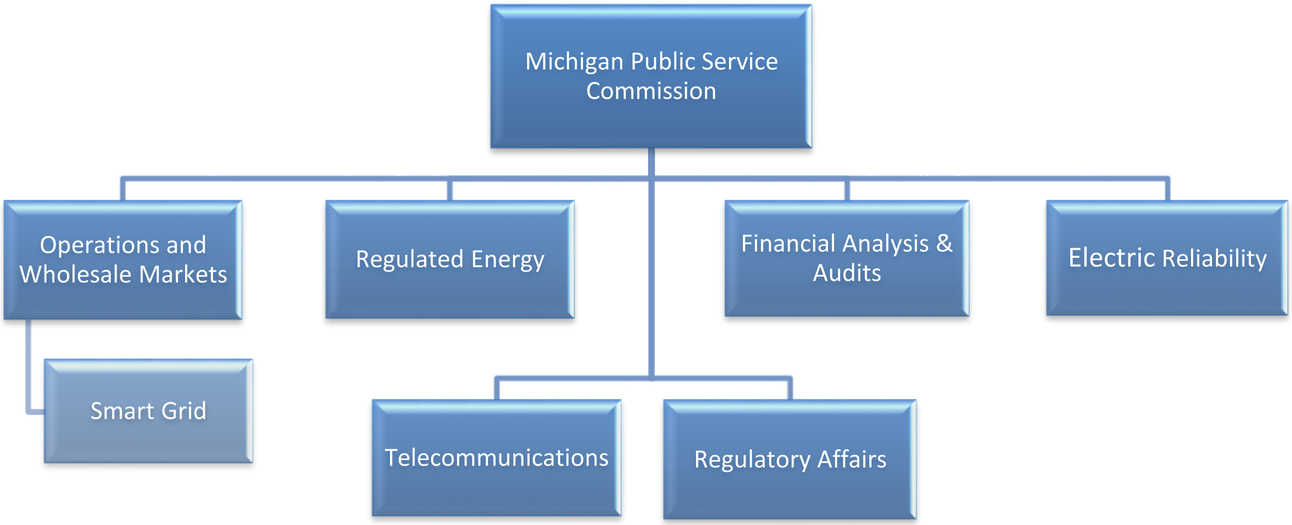
National Guard-Cyber Units/Michigan Department of Military and Veterans Affairs

The National Guard is a partner in many of the previously-described state efforts. As part of this work, the Guard is developing cyber units that have the skills and operational capabilities to further support this mission. These units include Michigan's Joint Cyber Operations Team, comprised of Army CND-T (8 PAX) in Lansing, the Air Cyber Team (7 PAX) in Battle Creek, and the Air Information Operations Platform. As previously noted, the 110th Airlift Wing National Guard Base in Battle Creek and the Joint Maneuver Center at Camp Grayling now has operational access to the Michigan Cyber Range for testing, training, and exercises. Signals capabilities exist within the Three Army Brigade Signal Company and the Four Air Communications Element and provide an additional building block for the Guard's future cyber force structure. As these capabilities continue to expand, future staffing needs are expected to be increasingly drawn from the National Guard Reserve versus active Guard units. This means that individuals that serve in the Reserves and that work in the private/public sector in cybersecurity can be utilized to support this efforts at a cost that would be less than maintaining the capability within the active Guard units.

[21] Michigan Executive Office of the Governor. Michigan Cyber Initiative – Defense and Development for Michigan Citizens Businesses and Industry. Page 7. Accessed on November 17, 2014. http://www.michigan.gov/documents/cybersecurity/MichiganCyberInitiative2011_365631_7.pdf

Michigan Public Service Commission/Michigan Department of Licensing and Regulatory Affairs

According to the Michigan Public Service Commission's (MPSC) *2014 Annual Report*[22], *"the mission of the Michigan Public Service Commission is to grow Michigan's economy and enhance the quality of life of its communities by assuring safe and reliable energy, telecommunications, and transportation services at reasonable rates."* As part of its mission, the MPSC is tasked with assuring the security of the state's critical infrastructure by promoting homeland security, promoting the state's economic growth, and enhancing the quality of life of its communities through adoption of new technologies (e.g., broadband telecommunications).


Michigan Public Service Commission
Operations and Wholesale Markets
Regulated Energy
Financial Analysis & Audits
Electric Reliability
Smart Grid
Telecommunications
Regulatory Affairs

The MPSC is organized into six divisions. The responsibilities for cybersecurity largely fall within the Smart Grid Section, which is housed in the Operations and Wholesale Markets Division: The Smart Grid Section is responsible for the oversight of utility implementation of smart grid technologies including the required cybersecurity safe-guards. When conducting analyses or prior to promulgating a position on cybersecurity issues, Smart Grid staff routinely collaborate with other MPSC sections, including the Electric and Gas Operations sections, as well as the Emergency Management Section of the Michigan Agency for Energy.

In 2013, the MPSC released the *Michigan Energy Assurance Plan*[23] which includes a cybersecurity component prepared by MPSC staff. The section states:

> *"Information and communications technology performs key functions in the production, transmission and distribution of energy and acts as the central nervous system of the electric, oil and natural gas infrastructure in North America. With an*

[22] Michigan Public Service Commission. 2014 Annual Report Page 4. March 2, 2015. Accessed on September 14, 2015. http://www.michigan.gov/documents/mpsc/2014_MPSC_Annual_Report_482786_7.pdf
[23] Michigan Public Service Commission. Michigan Energy Assurance Plan. Page 85. November 2013. Accessed on November 18, 2014.

> *ever-growing dependence on communication networks (hardware and software), there is an urgent need to protect energy control systems from cyber-attacks and accidents that could result in significant interruption of economic activities, and in worst cases, have large implications on public health and safety. As smart grid projects and plans have been implemented over the last few years, there has been increasing awareness of the risk of cyber-attacks and incidents within the electric industry. The growing concern has forced the industry to draft new regulations and standards in order to protect the networks and control systems from malicious attacks and accidental occurrences.*
>
> *MPSC staff reviewed multiple cybersecurity related documents published by the leading cyber security associations and found in common the following opinions:*
>
> - *Cyber security efforts should concentrate on rigorous open standards and guidelines through public-private partnerships for security,*
> - *Effective cyber security will rely on data sharing and cooperation between regulatory, private and electric industry entities,*
> - *A risk-based approach to cyber security planning should be implemented,*
> - *A cyber security performance accountability system should be created to fulfill risk-based planning, and*
> - *Regulatory bodies should be in constant contact with asset owners regarding cyber security."*

On January 12, 2012, the MPSC issued an order in Case No. U-17000[24] to launch an investigation into the deployment of smart meters by regulated electric utilities in the state. The order directed utilities to provide information to the MPSC by March 16, 2012, regarding their plans for smart meter deployment including proposed costs and benefits, scientific information addressing the safety of smart meter deployment, assurance of customer data privacy, and other information.

As part of this case MPSC Staff prepared a report[25] that was issued on June 29, 2012, which responded to both public comments submitted in the case and provided further analysis based on other studies and research. The report also contained a set of recommendations specifically related to cybersecurity, stating:

- *"Each utility should adopt an annual independent security audit of the mechanisms of customer access, third party access and internal cyber risk-management practices.*
- *As outlined in the NARUC resolution[26] regarding cyber security, the Staff intends to maintain a dialogue with regulated utilities to ensure that they are in compliance with standards, and that preparedness measures are employed to deter, detect and respond to cyber-attacks and to mitigate and recover from them.*

[24] Michigan Public Service Commission. Case U-17000. January 12, 2012. Accessed on November 18, 2014. http://efile.mpsc.state.mi.us/efile/docs/17000/0001.pdf

[25] Michigan Public Service Commission. U-17000 Report to the Commission. Page 28. June 29, 2012. Accessed on November 18, 2014. http://efile.mpsc.state.mi.us/efile/docs/17000/0455.pdf

[26] http://www.naruc.org/Resolutions/Resolution%20on%20Cybersecurity1.pdf

- *Utilities should adopt the same breach notification policies as other states have adopted, namely the notification of any breach affecting 1000 or more customers within two weeks of the breach.*
- *Each utility should be required to file a yearly breach notification summary with the Staff, detailing all breaches of customer information, including any third party breach information."*

To date, the Commission has not acted upon the staff recommendations on cybersecurity through an order. The Commission has, however, supported staff efforts to increase communication with both regulated and non-regulated critical infrastructure providers about cybersecurity best practices. The Commission has recently designated a full-tine staff position to serve as a liaison to utilities on cybersecurity matters. In 2013 and 2014, staff hosted two "Michigan Critical Infrastructure Stakeholder Cybersecurity Forum" events where critical infrastructure stakeholders in the state have jointly met to discuss and take action on cybersecurity issues. A third forum, this time co-planned with the Michigan Agency for Energy, will be held in late 2015.

Regarding data privacy, in Case No. U-17102 the Commission put forth a framework[27] designed to shape utilities' customer data usage and protection policies. After allowing a period of comment and review, the Commission ordered three of the state's largest utilities to file data privacy tariffs with the Commission. These tariffs, filed by DTE Electric Company, DTE Gas Company, and Consumers Energy Company, were approved by the Commission on October 17, 2013. With the release of the order MPSC Chairman John Quackenbush stated:

> *"Utility customers have a reasonable expectation of privacy related to the information that utilities collect, maintain, and disclose, including energy usage data and information provided by some customers that is used for the implementation and evaluation of various utility programs;"*
>
> *"The tariffs approved today limit the collection, use or disclosure of any customer information to accomplishing primary utility purposes only. The utility must obtain informed consent from the customer in advance in cases where the utility wishes to collect, use or disclose customer information for a secondary, non-utility purpose."*[28]

The order also directs the utilities to display a link to the customer data privacy tariff prominently on their respective websites within thirty (30) days.

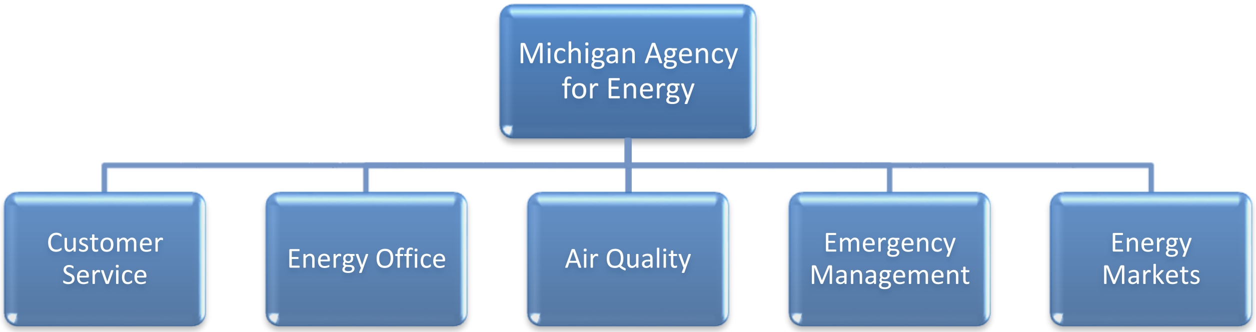
Michigan Agency for Energy/Michigan Department of Licensing and Regulatory Affairs

A newly formed entity, the Michigan Agency for Energy (MAE) was created by Governor Snyder through Executive Order No. 2015 – 10. The order, dated March 18, 2015, drew from state government a number of energy-related staff and consolidated them into one

[27] Michigan Public Service Commission. Case U-17102. October 31, 2012. Accessed on September 15, 2015 http://efile.mpsc.state.mi.us/efile/docs/17102/0001.pdf

[28] Michigan Public Service Commission. MPSC Approves Customer Information Privacy Tariffs for DTE, Consumers Energy. October 17, 2013. Accessed on November 18, 2014. http://www.michigan.gov/mpsc/0,4639,7-159-16400_17280-314865--,00.html

agency, with the purpose of establishing a centralized unit which will administer energy programs and serve as the focal point for state energy policymaking. In addition to its ancillary administrative, legislative, and communications staff, MAE consists of five functional groups which are organized as follows:



The Agency's lead unit on cybersecurity issues is the Emergency Management Section. The Section employs one full-time cybersecurity analyst, a full-time IT liaison, as well as other experts who are trained in the principles of emergency response and critical infrastructure protection, Cybersecurity responsibilities within MAE's Emergency Management Section include:

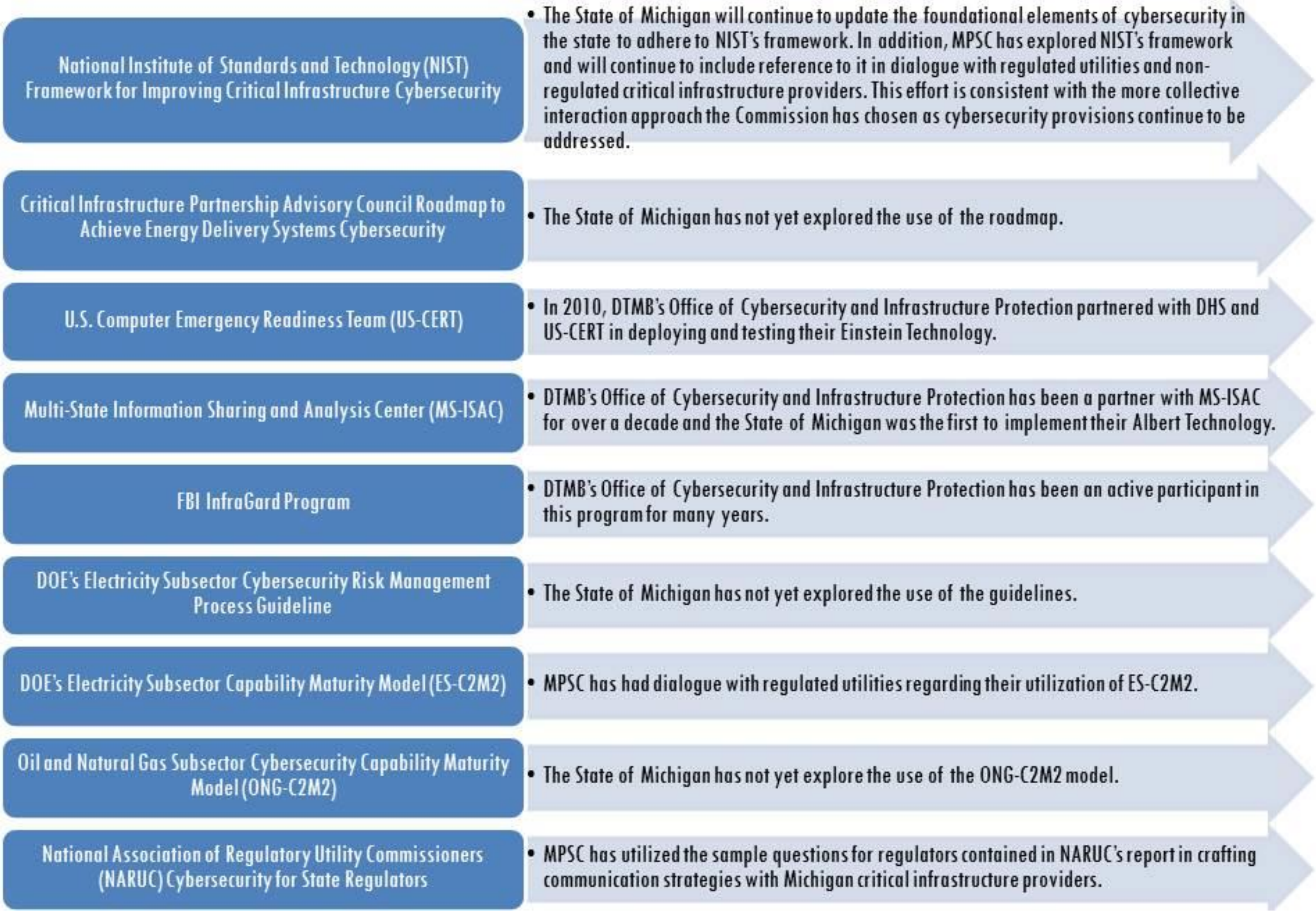
- Researching and reviewing current and proposed utility cybersecurity practices and assessing their impact on existing electric and natural gas systems.
- Assisting and providing guidance to MAE and MPSC staffs regarding cybersecurity issues and providing expert testimony in MPSC proceedings as appropriate.
- Developing and maintaining energy emergency response plans which incorporate the unique characteristics and spillover effects endemic to a cyber-attack.
- Collecting, managing, and disseminating cybersecurity information where appropriate.
- Helping plan and promote opportunities for MAE and MPSC staff to engage in cybersecurity training and interact with cybersecurity practitioners in Michigan.

Other units within MAE play an important role in fostering good cybersecurity in Michigan. The Energy Office, for instance, regularly serves as an agent in support of prudent cybersecurity practices. The Office is exploring including language in its grants and contracts, particularly for those projects which have IT components, which assures that appropriate cybersecurity measures are taken into account. This might include, for example, whether energy management systems supported by government funding have appropriate levels of cybersecurity embedded in their design and whether a process is in place to assure that these systems undergo regular software updates and security assessments.

Michigan Economic Development Corporation

As part of its overall mission, the Michigan Economic Development Corporation (MEDC) works with businesses in the state to develop new market opportunities and to help new businesses grow and thrive. As part of this mission, the MEDC focuses on attracting both cybersecurity businesses and the talent needed to support those businesses. As the need for cybersecurity has grown, so too have the business opportunities, and the MEDC has proven pivotal in enabling the development of cybersecurity firms in Michigan. The MEDC is also a partner in the Michigan Cyber Range and has made, and will continue to make, incremental investments to expand the Cyber Range and support economic cyber growth in Michigan.

State of Michigan's Efforts to Integrate Federal Cybersecurity Initiatives



National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity	• The State of Michigan will continue to update the foundational elements of cybersecurity in the state to adhere to NIST's framework. In addition, MPSC has explored NIST's framework and will continue to include reference to it in dialogue with regulated utilities and non-regulated critical infrastructure providers. This effort is consistent with the more collective interaction approach the Commission has chosen as cybersecurity provisions continue to be addressed.
Critical Infrastructure Partnership Advisory Council Roadmap to Achieve Energy Delivery Systems Cybersecurity	• The State of Michigan has not yet explored the use of the roadmap.
U.S. Computer Emergency Readiness Team (US-CERT)	• In 2010, DTMB's Office of Cybersecurity and Infrastructure Protection partnered with DHS and US-CERT in deploying and testing their Einstein Technology.
Multi-State Information Sharing and Analysis Center (MS-ISAC)	• DTMB's Office of Cybersecurity and Infrastructure Protection has been a partner with MS-ISAC for over a decade and the State of Michigan was the first to implement their Albert Technology.
FBI InfraGard Program	• DTMB's Office of Cybersecurity and Infrastructure Protection has been an active participant in this program for many years.
DOE's Electricity Subsector Cybersecurity Risk Management Process Guideline	• The State of Michigan has not yet explored the use of the guidelines.
DOE's Electricity Subsector Capability Maturity Model (ES-C2M2)	• MPSC has had dialogue with regulated utilities regarding their utilization of ES-C2M2.
Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2)	• The State of Michigan has not yet explore the use of the ONG-C2M2 model.
National Association of Regulatory Utility Commissioners (NARUC) Cybersecurity for State Regulators	• MPSC has utilized the sample questions for regulators contained in NARUC's report in crafting communication strategies with Michigan critical infrastructure providers.

Conclusion

NASEO held a series of meetings with personnel involved in Michigan's cybersecurity programs and initiatives to discuss how the state, through strong leadership from its Governor and through public-private collaborations, is addressing cybersecurity. Participants also discussed Michigan's cybersecurity model in the context of individual agency roles and responsibilities along with the state's response to the various federal efforts to improve cybersecurity. During the meeting the following key points and issues were identified:

1. Planning was underway to look at current and emerging cyber risks and develop a comprehensive plan that will guide the future of cybersecurity in Michigan As part of this effort, the state is looking to build the next generation of higher speed networks which will improve the state's capabilities to better detect and respond to threats.. This plan, titled the *Michigan Cyber Initiative 2015,* was completed and issued in November 2014. In addition, in October 2015, a Cyber Disruption Response Plan prepared by the Department of Technology Management & Budget was released to keep pace with the evolving natures of the cyber threat.

2. All state agencies have a role to play and the state can improve its capabilities to assure essential services through Continuity of Operations Plans.

3. The state is working to implement NIST's voluntary framework, but it is unclear to what degree it is scalable to smaller companies.

4. Information sharing between the public and private sectors continues to present challenges. Legal authorities to protect sensitive information need to be explored and trusted relationships with the private sector must be strengthened. Private sector companies must understand the need to share critical cyber infrastructure information with authorized public agencies. The public sector needs to better understand what information is being shared across the private sectors, which may necessitate the use of confidentiality and/or other agreements.

5. The state, with the assistance of larger utilities, needs to reach out to smaller utilities including electric, telecommunications, and water that may not have the resources to fully invest in cybersecurity.

6. NASEO, through an update of the Energy Sector Specific Plan, could help address some of these needs and encourage greater private sector coordination. NASEO has worked with other organizations (e.g., Edison Electric Institute, Electric Power Research Institute, American Public Power Association, American Gas Association, American Petroleum Institute, etc.) on this issue.

7. There is a need, from a national policy perspective, for federal legislative solutions, including an approach to the reporting of successful cyber-attacks (breach notifications).

8. There were questions on what the national labs are currently doing in regards to cybersecurity and how can their efforts be shared with states.

9. It was suggested that NASEO's work should be linked to the Naval Post Graduate School which does briefings for new governors on cyber threats.

10. It was also suggested that NASEO identify three (3) things that everyone agrees needs to be done now. For example, the need to assure that all sensitive data is encrypted had been a major focus. It cost the State of Michigan approximately $4 million to encrypt 90 percent of it sensitive data which has dramatically reduced the consequences of any potential data breach. NASEO should consider taking a similar approach to its *"10 Things Every Governor Should Know for Energy Assurance"* for cybersecurity.

NASEO will continue to support federal cybersecurity initiatives while also encouraging states to develop cybersecurity framework models to ensure our nation's ability to prevent, respond to, and coordinate mitigation efforts against attacks to the nation's critical cyber and communications networks and infrastructure. NASEO will next be working with the State of Virginia to document steps they have taken to address cybersecurity. This work will provide states with opportunities to engage in peer information exchange sessions with the goal of increasing the states' capacity to deal with evolving cybersecurity threats.

***