“It takes a network to protect a network.”
September 16, 2013

Dear Michigan Critical Infrastructure Partners:

Every day, Michigan government detects tens of thousands of unauthorized attempts to probe, scan, and access or disrupt its computer networks. These same computer networks safeguard important information about Michigan’s residents, control critical state agency operating systems, and provide our customers with convenient access to state services. While the vast majority of these cyber anomalies are blocked by defensive systems, evolving threats represent a significant risk to the continuity of state government. Similar challenges are faced by Michigan’s private sector and local government partners, all of whom are also working diligently to safeguard their systems.

With the understanding that it takes a network to protect a network, Governor Rick Snyder introduced the Michigan Cyber Initiative to encourage a statewide effort among public and private partners to defend Michigan’s critical networks. In support of this Initiative, a team of state and local government representatives and private sector critical infrastructure owners and operators have developed the Michigan Cyber Disruption Response Strategy.

This document provides a framework for the prevention of, protection from, response to and recovery from a significant cyber disruption to Michigan’s critical infrastructure. Through the strategy and its operational annexes, participating organizations can collaborate in response to cyber threats either before or after they occur. The strategy sets forth a number of goals and objectives designed to provide an operational framework to respond to today’s cyber anomalies, as well as a cooperative approach aimed at preparing and maintaining a cadre of cyber security partners to maintain ongoing readiness.

It is our hope that by unifying state government cyber security efforts, and by working closely with our private sector and local government partners, we can continue Michigan’s role as a national model of innovation, success and security.

David Behen
Michigan Chief Information Officer

Colonel Kriste Kibbey Etue
Director, Michigan State Police

Major General Gregory J. Vadnais
Adjutant General, Michigan National Guard
## Contents

- Purpose, Scope, and Methodology ................................................................. 1
- Problem Definition and Risk Assessment ....................................................... 1
- Goals, Objectives, and Performance Measures ............................................. 2
- Resources and Investments ........................................................................... 4
- Organizational Roles, Responsibilities, and Coordination ........................... 5
- Integration and Implementation ................................................................. 6
- Conclusion ...................................................................................................... 7
Purpose, Scope, and Methodology

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 the State of 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.

The Michigan Cyber Disruption Strategy addresses significant cyber disruption events in the State of Michigan. A significant cyber disruption event is defined as “an event that is likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability, of electronic information, information systems, services, or networks; and/or threaten public safety, undermine public confidence, have a negative effect on the state economy, or diminish the security posture of the state.”

Problem Definition and Risk Assessment

In 2012, the State of Michigan’s governmental computer networks detected an average of 187,000 cyber anomalies every day. Critical state government systems are thus vulnerable to phishing emails, denial of service attacks, attempts at unauthorized access, malware, probes and reconnaissance scans and other malicious intrusions. The same issues are affecting critical infrastructure owners throughout the state and the nation.

State and local governments and critical infrastructure owners and operators must understand their respective vulnerabilities in order to reduce risk to their systems and operations. Moreover, these critical service providers must understand their collective vulnerabilities caused and propagated by the unique interdependencies present in the realm of critical infrastructure. Risk of service interruptions can be mitigated by coordination and collaboration with other public and private partners that provide critical services to the public.

1 Definition derived from the National Cyber Incident Response Plan, Interim Version, dated September 2010.

2 Statistic provided by the Michigan Department of Technology, Management and Budget, Cyber Security and Infrastructure Protection Administration (CIP), Michigan Cyber Security Office.
Goals, Objectives, and Performance Measures

The primary goal of this strategy is to ensure that no critical service in Michigan is significantly impacted by a cyber-attack. However, understanding the complexity of systems and networks, and the limitations in resources that exist in every organization, we have created a series of achievable goals and objectives designed to achieve maximum results.

**Goal 1: Improve situational awareness among cooperating critical infrastructure owners and operators through enhanced communication and collaboration regarding cyber threats.**

- Objective 1.1 – Create a contact list of all participating critical infrastructure owners and operators and key stakeholders by October 2013.
- Objective 1.2 – Develop a system, agreed by all parties, to share information among members and stakeholders by December 31, 2013.
Goal 2: Create specific plans, as annexes to the strategy, for the prevention and mitigation of, response to, and recovery from cyber disruption events affecting critical infrastructure owners and operators by 2014.

- Objective 2.1 – Develop a consensus-driven response plan template for use by all members and stakeholders by December 31, 2013.
- Objective 2.2 – Develop owner/operator specific response plans for cyber disruption events using the consensus template by December 31, 2014.

Goal 3: Train key staff and exercise communication and response plans developed in accordance with this strategy annually, beginning in 2013.

- Objective 3.1 – Develop a consensus-driven training plan for members and stakeholders by December 31, 2013.
- Objective 3.2 – Develop an exercise plan for implementing the strategy by December 31, 2013.
- Objective 3.3 – Conduct exercises of at least one component of the cyber disruption strategy annually.

Goal 4: Conduct thorough risk assessments to identify the vulnerabilities of Michigan’s critical infrastructure to cyber-attack.

- Objective 4.1 – Each critical infrastructure owner/operator will develop a risk assessment of its networks by December 31, 2014.
- Objective 4.2 – Develop a remediation plan based on the risk assessment priorities by July 31, 2015.
- Objective 4.3 – Apply resources to the remediation of identified vulnerabilities and report outcomes by December 31, 2015.
- Objective 4.4 – Re-evaluate risk assessments for all systems every 3-5 years.
The major milestones of this strategy will be the completion of the individual goals and objectives. In addition to monthly coordination meetings or teleconferences, a conference of the strategy’s participants will take place each September and an annual report will be published to keep stakeholders informed of milestones and progress.

Resources and Investments

The success of this strategy, and its reach, is dependent upon the voluntary resources applied to its implementation by participating critical infrastructure owners and operators and government agencies. In the case of private sector critical infrastructure owners and operators, corporate members must make a concerted effort to apply resources to meet the goals and objectives as part of their businesses’ overall security investment. However, it is understood that any resources applied to contribute to the state’s cyber disruption strategy will necessarily be applied in ways that support the private sector’s responsibilities to owners and shareholders. Therefore, a key role of the private sector members of this strategy will be to identify and communicate innovative solutions for implementing these goals in ways that demonstrate the benefits to their customers and shareholders.

Governmental members of the strategy must apply the “tools of government” to the completion of the strategy’s objectives. These “tools” include appropriated fiscal resources, standards, incentives, and regulations designed to support the goals and objectives of the strategy. Ultimately, government has the unique responsibility to lead, participate in, and support this strategy concurrently.
Organizational Roles, Responsibilities, and Coordination

This strategy is designed to be implemented by the participating members. To be successful, any collaborative initiative must have an owner or director that ensures participation, reports on progress, oversees the framework and engages new members. As such, the State of Michigan Chief Security Officer and the Michigan Department of Technology, Management and Budget will be 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 and the coordination of the protection of Michigan’s critical infrastructure.
The next section of the strategy provides the framework for the ongoing development of plans designed to provide specific response protocols for members of the Michigan cyber disruption strategic initiative. These plans, which will be added to the strategy as annexes, constitute the ongoing work of the participants. To facilitate this work, it is recommended that a rotational chairperson be designated in one-year terms. This individual and their associated organization will coordinate regular meetings, facilitate progress on specific plans, and oversee the group’s operational activities for their given term.

Integration and Implementation

The Michigan Cyber Disruption Response Strategy is designed to serve as an ongoing framework for collaborative response to significant cyber events. The document is understood to be continually evolving, and the primary component of that evolution will be the ongoing development of specific plans for prevention of, response to and recovery from significant cyber disruptions. As a first priority, members will develop a written plan for communication during cyber events.

Initially, the group will develop the content of the first annex, the Communication Annex, which will provide the necessary framework for communication among critical infrastructure owners and operators and government within Michigan. The Communication Annex will include the protocols for communicating among members, as well as to stakeholders, to mitigate the effects of cyber disruption.

Following the completion of the first annex, strategy participants will develop specific plans for their response to cyber disruptions affecting their critical infrastructure. As part of this planning process, critical infrastructure owners and operators will collaborate to identify specific interdependencies that exist within and without their respective sectors. In doing so, the unique vulnerabilities associated with these sectors will be identified and plans developed to address interdependencies as a key component of the planning process. To ensure that protected critical infrastructure information is not released, information must be safeguarded. As such, the annex may contain references to documents that are privately held by individual members and not available for public distribution with the strategy.
The third annex will provide specific training recommendations for members of the strategic partnership with employees active in cyber disruption mitigation. These training recommendations will be customized for individual positions and their core competencies related to cyber security. In addition, the third annex will contain an exercise plan for the overall strategic initiative which will begin with drills and tabletop-level exercises in 2013, and culminate in a full scale exercise within 5 years.

The final annex addresses the foundational need to understand the risk associated with cyber disruptions to critical facilities. An improved understanding of the threats, vulnerabilities and potential consequences of cyber disruptions to Michigan’s critical infrastructure will result in more effective scenario-based response plans. In accordance with the Michigan Emergency Management Act (PA 390 of 1976) and in recognition of national policy including Presidential Policy Directive 21 and Executive Order 13636, Michigan will lead the nation in the development of risk-based plans for managing cyber disruptions to critical systems.

Any cyber event that has the potential to substantially affect the State of Michigan, its residents, businesses or governments may result in the implementation of local or state emergency management plans.

**Conclusion**

Critical infrastructure systems are networks, and so are groups that attack them. It follows that the best way to respond is to develop a network designed to protect critical infrastructure. Since it is not possible to protect every component of every network, efforts must be undertaken to protect the “critical nodes” identified through careful risk assessment and collaborative analysis of interdependences. The Michigan Cyber Disruption Response Strategy is the first step in the development of a force-positive network designed to apply risk-based mitigation strategies to the defense of critical infrastructure. The subsequent steps will be the detailed development of plans and procedures to assess risk, communicate threats, issue protocols and train and exercise staff in the protection of Michigan’s critical infrastructure from significant cyber disruptions.
Communication Annex
Introduction

Goal 1 of the Michigan Cyber Disruption Response Strategy is to “Improve situational awareness among cooperating critical infrastructure owners and operators through enhanced communication and collaboration regarding cyber threats”. In order to meet this goal, it is necessary to develop a protocol designed to aid in the informed use of communication and collaboration tools and to identify these tools and the means of accessing them. The Communication Annex provides this information.

Parameters for Activation

The activation of response activity via this protocol can cause unnecessary expense and business interruption if inappropriately employed. As such, a set of parameters have been developed for the proper use of the protocol. First, two scenarios have been envisioned for the use of the Michigan Cyber Disruption Response Strategy Communication Protocol. These are:

1. A cooperating member of the strategic partnership has experienced, or is experiencing, a harmful cyber disruption due to a novel cyber anomaly and has a demonstrated need to issue a warning or request assistance; or,

2. A cooperating member would like to share important information regarding emergent cyber anomalies or threats.

It is not currently anticipated that the protocol will be employed outside of these parameters. However, changes to these and other parameters within this annex are at the discretion of the members.
Authorized Agents

Each member of the strategic partnership shall identify an “authorized agent” that will act as the individual authorized by the partner entity to use this protocol. A list of authorized agents will be maintained as part of this annex by current chairperson of the strategic partnership. Authorized agents should be individuals authorized to request resources on behalf of their company or agency or to provide resource support to other partners. Notification under the partnership will be delivered to authorized agents only. Notifications issued by authorized agents will be classified according to one of the following classifications by the information owner:

1. Confidential – Authorized Agents Only;
2. Proprietary – Share within the member community only;

Information shared within the partnership shall remain the property of the information owner, and shall therefore not be reclassified by any other than the owner.

As a result of governmental involvement in the Michigan Cyber Disruption Response Strategy, certain documentation pertaining to activities undertaken by the strategic partnership could be subject to Freedom of Information Act requests. As such, it is recommended that all such requests be forwarded to the State of Michigan for review by state FOIA coordinators to ensure compliance with the applicable laws. It should be noted that certain documents, such as security sensitive information regarding members, may be exempt from disclosure under the act (Act 442 of 1976 (15.231 et seq.)). Section 13 of the Act specifically exempts from disclosure information relating to “domestic preparedness strategies” and provides other exemptions which may be applicable.
Cyber Disruption Response Strategy

Communication Protocol – Steps for Activation

The following steps should be followed in the event a member of the strategic partnership desires to activate the communications annex protocol:

1. An authorized agent shall initiate communication by calling the activation phone number.

2. An operator will verify the authorized agent using an authorization list and a unique passphrase.

3. The Authorized Agent shall make the report. The report should include the following at minimum:
   
a. Corporate Identity
   b. Authorized Agent Full Name
   c. Authorized Agent Phone Number
   d. Authorized Agent Email
   e. Issue Information:
      i. Describe the issue and its impact.
      ii. When was this issue discovered?
      iii. Is this issue an emergency, an important notification, or for information only?
   f. Are you requesting activation of the state government resources or other assistance? If so, explain.
   g. The State of Michigan Service Monitoring Center will do the following:
      i. Determine Action level:
         1. Level 1 (Emergency) - SMS/Text/Email, Phone Call and Conference Line
         2. Level 2 (Important Notification) - SMS/Text/Email and Automated Phone Call
         3. Level 3 (For Information Only) - SMS/Text Message/Email to Members
      ii. Log all relevant information:
         a. Describe what was done, time and dates in the appropriate field on the form.
A form for the collection of information from Authorized Agents for use by SMC operators is attached to this annex.

**Authorized Agent Contact List**

As indicated in the strategy, a rotational chairperson will be selected to manage the administrative duties associated with the partnership on an annual basis. This rotational chairperson shall be responsible for the management of the member contact list, as well as the Authorized Agent list. A template for the Authorized Agent contact list is attached as part of this Annex.

**Partnership Contact List**

The rotational chair shall also maintain, separate from the Authorized Agent list, a list of participants in the Michigan Cyber Disruption Response Strategy for the purposes of general communication regarding the partnership.
Cyber Disruption Response Strategy
Response Plans
Annex
Introduction

Based on the need to create a common operational picture among participating critical infrastructure owners and operators, this annex provides a template for the development of cyber response plans for Michigan’s critical infrastructure, and a framework for response to cyber disruptions. These efforts are based on the cyber incident response cycle, which describes the “fundamental elements of prevention and protection activities” associated with a cyber response³.

Within the Michigan Cyber Disruption Response Strategy, the theoretical elements of the cyber incident response cycle are recognized and integrated into a practical solution designed for daily use. The major components of the cycle are reflected in the key sections of the strategy. As part of this strategy, participants may engage in some or all of these components at their discretion.

Prevention and Protection

The key to the prevention and protection of critical infrastructure from cyber attack or disruption is trained and competent technical staff and managers. Security professionals in critical infrastructure operations must be trained in the latest tools and techniques for the defense of their networks against disruption.


⁴ ibid, p 25.
This strategy focuses its support for prevention and protection of critical infrastructure networks on providing state-of-the-art training opportunities for its members and participants. The Michigan Cyber Range, developed by the State of Michigan in conjunction with private partners, including Merit Networks, has developed a training curriculum for cyber security professionals. Located in Ann Arbor, Michigan, the Michigan Cyber Range was developed to provide not only world-class training, but also a safe and secure facility within which to practice, test and develop cyber security tools and techniques.

In addition to the Michigan Cyber Range, cyber security training opportunities are available from public and private sector sources. These are detailed in the strategy’s Training and Exercise Annex.

Detection and Analysis

Critical infrastructure owners and operators function in an environment that is necessarily carefully structured. Proprietary information is guarded and disclosed only to trusted partners for common benefit. Like many businesses, critical infrastructure operations, especially in the private sector, owe it to their stakeholders to safeguard critical information that is essential to the success of their business. As such, the detection of cyber anomalies and the effects of these anomalies must be disclosed voluntarily by the partners according to their needs.

The detection and analysis of cyber disruption within the strategy is developed via the Communication Annex. The strategy provides a framework within which participants can build the necessary “trusted partner” relationships. By implementing the protocol within the Communications Annex, participants may alert one another regarding cyber anomalies they have detected. Further, they can access a network of cyber security professionals within the critical infrastructure arena which can analyze the anomalies and provide critical information for the common benefit.
Response and Resolution

The goal of this annex is to provide a template for how critical infrastructure owners and operators can work together to respond to cyber disruptions, thus addressing the response and recovery, or resolution, components of the cyber incident response cycle. The following sets forth a framework, or template, for the development of specific cyber disruption response plans for critical infrastructure sites.

The Michigan Cyber Disruption Strategy Response Annex provides for four (4) separate and unique levels of response to cyber anomalies or disruptions. These four (4) levels of response govern the types of activities involved, the resources applied, and the level of partner engagement expected in response to the event.

<table>
<thead>
<tr>
<th>Response Level</th>
<th>Communication Activity</th>
<th>Anticipated Response Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level IA</strong> (Severe)</td>
<td>All Communications Coordinated via SEOC/Joint Information Center</td>
<td>State Emergency Operations Center activation. Coordination of a statewide response by the Michigan State Police.</td>
</tr>
<tr>
<td><strong>Level I</strong> (Substantial)</td>
<td>SMS/Text/Email, Phone Call and Conference Line Initiation</td>
<td>Voluntary resource collaboration between members, technical information sharing, and resource deployment based on mutual aid agreements. Could include financial considerations.</td>
</tr>
<tr>
<td><strong>Level II</strong> (Elevated)</td>
<td>SMS/Text/Email and Automated Phone Notification</td>
<td>Real time, synchronous collaboration via phone and email as required. No financial considerations, no deployments. All activities conducted remotely.</td>
</tr>
<tr>
<td><strong>Level III</strong> (Guarded)</td>
<td>SMS/Text/Email to Members</td>
<td>Informational only. No follow-up activity required. No real time collaboration. All information sharing activity is passive and asynchronous.</td>
</tr>
</tbody>
</table>

Table R-1: Michigan Cyber Disruption Response Levels and Anticipated Engagement Activities
The table is designed to serve as a guide for participants in the Michigan Cyber Disruption Response Strategy, as well as a template for the development of cyber response plans within Michigan’s critical infrastructure sector. Further, these four levels are intentionally integrated with the National Cyber Risk Alert Levels listed within the Interim Version of the National Cyber Incident Response Plan, which are Severe, Substantial, Elevated and Guarded.\(^5\)

**Response Plans Template**

In the development of cyber response plans within critical infrastructure facilities, the following response plan template is proposed based on the tenets of the Michigan Cyber Disruption Response Strategy:

1) Introduction
2) Background
3) Critical Systems Information
4) Concept of Operations
   a) Prevention and Protection
   b) Detection and Analysis
   c) Response and Recovery
5) Specific Cyber Response Action Plans
   a) Data Backup Action Plan
   b) Disaster Recovery / Business Continuity Plan
   c) Halt Key Processes Plan
   d) Equipment Shutdown Plan
   e) Log File Recovery Plan
   f) Communication Plan (Include Media, Executives, etc.)
   g) Michigan Cyber Disruption Response Activation Plan
6) Annexes - Forms, Applications and Equipment Information, etc.

Law Enforcement Response

During the detection and analysis of cyber incidents, critical infrastructure owners and operators may suspect or discover criminal activity. It is essential that in the process of defending public and private networks in the state that we also root out the criminal elements that perpetrate such crimes. To that end, the Michigan State Police have established the Michigan Cyber Command Center (MC3). The MC3 is a resource for Michigan residents, groups, businesses and governments for the reporting, investigation and eventual prosecution of groups and individuals that commit cyber crimes. Members of the MC3 are partners in the Michigan Cyber Disruption Response Plan. Cyber anomalies at any level that have a law enforcement nexus will be shared with the Michigan Cyber Command Center for possible investigation or analysis.
Training & Exercise
Annex
Introduction

While developing a thoughtful and well-coordinated response to a cyber disruption is essential to protecting critical infrastructure, preventing one from occurring at all is preferred. A key component of any prevention strategy is the deployment of expert personnel that are prepared with the tools necessary to maintain a high level of threat awareness, quickly detect and mitigate vulnerabilities, and minimize the consequences of cyber disruptions. Like any tool, the effectiveness of cyber security tools is enhanced when they are wielded by experts. Critical infrastructure owners and operators must train staff in cyber security skills, and exercise their teams regularly to protect their systems and respond to cyber disruptions that overcome defenses. The purpose of this annex of the Michigan Cyber Disruption Response Strategy is to develop a plan for training and exercising cyber security professionals charged with the defense of Michigan’s critical infrastructure.

Training Plan

A one-size-fits-all training program would not effectively serve the diverse membership of the Michigan Cyber Disruption Response Strategy. Michigan’s partnership uniquely includes public and private organizations of all sizes with vastly different priorities and resources. As such, the following training plan represents a set of recommended capabilities, each associated with a domain of cyber security that is essential to the protection of critical systems. The development of these capabilities within partner organizations is the goal. The form that those capabilities take within the organizations is up to the partners.

A basic concept of modern telecommunications is the Open Source Interconnection, or OSI, Model. The OSI is a concept that standardizes the interconnection of devices by creating a model of abstract layers. In recognition of the significance of this fundamental concept, and with the layers of the OSI model as a guide, the following represents the core training domains of cyber security for the purposes of the Michigan Cyber Disruption Response Strategy. It is essential that a critical infrastructure owner or operator ensure that expertise in these seven (7) primary areas of cyber security resides within their organization. The key topics within each domain are also listed to indicate the types of information to be covered within each domain. They are not intended to be all inclusive.
1. Application Level Security
   a. Known Software/Database Vulnerabilities (Java, SQL)
   b. Web Application Security
   c. Application Based Attacks (Buffer Overflow, SQL Injection)
2. Hardware and Device Level Security
   a. Vulnerabilities of Routers, Switches, Servers
   b. Cryptography
   c. Firewalls
3. Network Level Security
   a. OSI Model and Protocols
   b. Network Architecture (LAN, Wireless)
   c. Network Based Attacks (wireless intercept, IP spoofing)
4. Disaster Recovery and Business Continuity
   a. Business Impact Analysis
   b. Business Continuity Planning
   c. Interdependency
5. Computer Forensics
   a. Seizure Concepts
   b. Incident Investigation
   c. Digital Evidence and Electronic Discovery
6. Physical Security
   a. Risks, Threats and Countermeasures
   b. Physical Intrusion Protection
   c. Access Control
7. Incident Management
   a. Incident Command System
   b. Roles and Responsibilities
   c. Incident Reporting
Training Resources

Michigan is uniquely equipped to train its cyber security experts. In 2011, Governor Rick Snyder launched the Michigan Cyber Range as an integral part of Michigan’s Cyber Initiative to protect families, communities, businesses and government. Located in Ann Arbor, Michigan at the offices of Merit Networks, the Michigan Cyber Range offers a unique venue for information technology training that allows students to test their skills in a safe and realistic environment.

The Michigan Cyber Range offers a number of courses that provide training in the six domains of the Michigan Cyber Disruption Response Strategy. The following provides a list of the courses and certifications appropriate for the purpose of this training plan. As before, this list is not intended to be all-inclusive:

1. Application Level Security
   a. Certified Information Systems Security Officer
   b. Certified Penetration Testing Consultant
   c. Certified Penetration Testing Engineer

2. Hardware and Device Level Security
   a. Certified Information Systems Security Officer
   b. Certified Penetration Testing Consultant
   c. Certified Penetration Testing Engineer

3. Network Level Security
   a. Certified Information Systems Security Officer
   b. Certified Penetration Testing Consultant
   c. Certified Penetration Testing Engineer

---

4. Disaster Recovery and Business Continuity  
a. Certified Disaster Recovery Engineer

5. Computer Forensics  
a. Certified Network Forensics Engineer  
b. Certified Digital Forensics Examiner

6. Physical Security  
a. Certified Information Systems Security Officer

7. Incident Management  
a. Certified Incident Handling Engineer

These courses are offered throughout the year at the Michigan Cyber Range. More information and a course listing are available at www.merit.edu/cyberrange.

In addition to the Michigan Cyber Range, a variety of public and private organizations provide training in the domains listed in the previous section. These include:

• Federal Emergency Management Agency (FEMA) Emergency Management Institute (EMI) – Offers a variety of in residence and online courses in incident management, security and emergency management, including several on continuity and disaster recovery (www.training.fema.gov).

• The SANS Institute – Specialized information technology training resources delivered in a variety of formats (www.sans.org).

• International Information Systems Security Certification Consortium (ISC²) – Offers a number of training and certification options including the industry leading Certified Information Systems Security Professional (CISSP) designation (www.isc2.org).

**Cyber Disruption Exercise Strategy**

In order to maximize the momentum gained by this partnership, an aggressive plan is proposed for exercising the Michigan Cyber Disruption Response Strategy. The members, according to the third goal of the strategy will develop an exercise plan by the end of 2013. The exercise doctrine will follow that of the Department of Homeland Security’s Homeland Security Exercise and Evaluation Program (HSEEP). HSEEP ensures that exercises are conducted...
according to a standard methodology which is risk-based and applicable to all mission areas; prevention, protection, mitigation, response and recovery. The HSEEP methodology is summarized in the following graphic:

HSEEP Exercise Cycle

Exercise Plan

The following represents the plan and schedule developed by the membership to meet goal three (3), objectives 3.2-3.3 of the plan. The exercises are progressive according to the HSEEP doctrine. The specific dates and outcomes will be updated in subsequent editions of the strategy to reflect changes and confirm accomplishments:

2. Michigan Cyber Security Table Top Exercise (TTX) – October 2013
5. Michigan Cyber Security Annual Exercises – Fall Annually

Risk Assessment Annex
Introduction

Michigan’s critical infrastructure systems are vast, interconnected, interdependent networks. No single entity, public or private, can afford to apply the resources necessary to eliminate all threats to continuity. A public-private partnership, like that represented by the Michigan Cyber Disruption Response Strategy, can leverage the resources of multiple stakeholders to gain advantage, but even this falls short of total risk elimination. These limitations therefore require the development of a method to assess and prioritize risks in order to focus resources on the most critical areas of Michigan’s networks. This annex provides a framework for the assessment and management of the risk of disruption of Michigan’s critical infrastructure networks.

Risk Management Framework

The National Infrastructure Protection Plan (NIPP) was developed by the US Department of Homeland Security as a strategy for the protection of national critical infrastructure. Within the NIPP, a risk management framework has been established to provide a common operational picture for the management of risk to critical infrastructure. The State of Michigan supports the National Infrastructure Protection Plan. Hence, any state-level risk management strategy should build upon this foundation and support the overall effectiveness of the national plan.

The adopted risk management framework for the Michigan Cyber Disruption Response Strategy is represented in the following graphic:

Each step of the framework is a key component of Michigan’s overall cyber disruption risk management strategy. The Michigan Cyber Disruption Response Strategy sets goals and objectives for the management of cyber disruptions affecting critical systems. The remaining areas of the risk management framework are equally important to the effective management of cyber disruption risk.

Identification of Network Components

The first critical step in the assessment of risk to critical networks is the identification and inventory of network components or assets. The development of a comprehensive inventory of logical infrastructure can be challenging, especially when compared to inventory of physical assets such as buildings. Nevertheless, it is only via the identification of the critical components of a network that one will be able to understand the associated threats and vulnerabilities. The asset’s position, connectivity, and other unique characteristics relate directly to their criticality and vulnerability.

The identification and inventory of network components should include special attention to highly concentrated groups of network assets. These “hubs” represent critical nodes that are typically highly connected to other areas of the network and thus highly vulnerable. In other words, these critical nodes represent the place where attacks can do the most damage. By protecting critical nodes of a network, applied resources can have the greatest return on investment (ROI). Critical nodes can be identified by comparing the connectivity of hubs to other areas of the network via the inventory. Critical nodes can also be uncovered as a result of risk assessments that identify high consequence assets, by penetration testing, and by experts in network architecture.

Risk Assessment Methodology

Risk assessment involves the development of a measure of risk based on the evaluation of the threat, vulnerability and consequence associated with an attack on a target, such as critical infrastructure. Risk assessment is necessary for risk management and typically involves the following steps:

1. Identify critical infrastructure and key resources;
2. Identify and assess threats to the subject infrastructure;
3. Identify the vulnerabilities of the target infrastructure associated with the identified threats;
4. Evaluate the consequences of a successful attack on the subject infrastructure;
5. Determine the risk to the subject infrastructure based on the aforementioned factors;
6. Identify means of reducing risk to subject infrastructure;
7. Evaluate the resources available to mitigate risk; and,
8. Develop a risk management strategy taking into account the risk priorities and resources available.

Common methods for risk assessment include the use of subject matter experts and the scoring of risk characteristics based on relativistic scales. Additionally, penetration testing or “red team” techniques may be used to uncover vulnerabilities and test security of potential targets, yielding data that may be used to develop risk assessments and mitigation priorities.

A common method of risk evaluation is the use of relativistic methodologies. In this approach, various scales are used commonly across all evaluated targets and targets are given a score based on the assessor’s determination. Often, these risk assessments are conducted by individuals with expertise in the given sector in order to support the evaluation’s integrity. These scales are typically represented in one of two ways, either by a scoring scale which applies points to different vulnerabilities which are later totaled, or by percentage. In the case of percentage the decision factor is often represented as (0,1), meaning the factor should be rated as 0% probably (0) to 100% probable (1). For example, the threat of a vehicle borne improvised explosive device at a particular target site may be assessed by an expert to be 85% likely (.85). The factor can then be applied in a formula upon which the method is based.

\[
R = TxVxC
\]

Where:
- \( R \) = Risk (Expected Loss)
- \( T \) = Threat
  - (0,1)
  - Likelihood of a potential type of attack
  - Intent and capability of the adversary
- \( V \) = Vulnerability
  - (0,1)
  - Likelihood or probability of successful attack
- \( C \) = Consequence
- Replacement cost, could be in dollars
- Direct economic impact
- Indirect economic impact

The Michigan Cyber Disruption Strategy does not mandate a risk assessment methodology. Instead, it recommends that any risk assessment developed by partners is documented, reproducible, and defensible and based on the risk factors indicated above. The hope is that risk assessment results can be discussed and shared with partners, as appropriate, to assist in the identification of critical network nodes and their associated interdependencies.

Prioritized Remediation

Ultimately, the goal of the risk assessment process is to provide a prioritization of the critical assets of Michigan’s networks, and a plan to safeguard them. The highest priority assets should be those that are most vulnerable and would have the greatest impact if disrupted. As such, these critical nodes should receive the greatest amount of resource support. Members will develop remediation plans based on their risk assessment activities by December of 2015. These plans will be reported to the partnership at a level of detail deemed appropriate by the reporting member.

It is envisioned that, where possible, partners of the Michigan Cyber Disruption Strategy will share information about their highest priority assets. The identification of critical nodes within Michigan’s critical infrastructure networks will allow the State of Michigan and its partners to better manage resources to protect critical systems. Additionally, training and exercise programs can be tailored to target the protection of these critical assets.

Measuring Effectiveness

An effective protective program should yield measurable progress. Regular meetings of the Michigan Cyber Disruption Response Strategy Partners held after 2015 (when remediation plans are developed) will include a structured report of the effectiveness of remediation. These reports will include, at minimum, a total number of successful disruptions and a measurement of any applicable reductions in disruptions of critical networks associated with the remediation activities undertaken.