Appendix I

Cyber Security

Table of Contents

Additional appendices referenced in the
Cyber Security plan are available upon request

Dan Lohrmann
Director, MDIT Office
of Enterprise Security,
State of Michigan CISO

An "all hazards" approach is helping us effectively manage emergencies and keep the business of state government—critical IT services to Michigan citizens—running smoothly.

Vision of Action

The Cyber Security Strategic Plan began with an in-depth review of our systems and procedures, involving a wide cross-section of Michigan's state government. To ensure we were meeting business needs, we spoke first with our customers, beginning with state agency senior executives. We were able to include perspectives of the business, technical and executive-leadership to develop state-of-the-art, customer-focused solutions. We also benefited from external analysis of our practices and opportunities for advancement.

The end product is something we can be proud of; it is something that will carry the work of the Michigan Department of Information Technology (MDIT) into the future. It will help us reach our vision of being a recognized leader in providing best-practice security solutions to protect the privacy and information of Michigan's citizens.

This document illustrates our philosophy for the future, which is centered on risk reduction, business continuity, training and culture and a commitment to excellence. We are proactively protecting networks and communication as well as the data that have been entrusted to us. We are accomplishing this through deployment of technology to our agency clients and developing partnerships with the larger security community, including federal, state and local experts and stakeholders.

Our vision of action will ensure that we can effectively handle recovery from all types of disasters. An "all hazards" approach is helping us effectively manage emergencies and keep the business of state government—critical IT services to Michigan citizens—running smoothly. Finally, we are equipping state employees with training and a solid understanding of their roles and responsibilities in protecting citizen information and maintaining the highest ethical standards.

As we look forward, we realize that change will continue to occur. Our security approach enables us to adapt to changes in the risk environment. To this end, we are developing new policies and procedures, including a template for state agencies to use in developing security plans. We invite you to join us on this important journey into the future of enterprise security.

Guiding Principles

Our vision of being recognized leaders in providing best-practice security solutions is central to everyday operations of the Office of Enterprise Security (OES). Together with our partners, we are working to ensure the confidentiality, integrity and availability of State of Michigan information assets. Security awareness is a vital piece of this work.

Our paramount and daily mission is to successfully carry out security operations and oversight in concert with our Michigan Department of Information Technology (MDIT) partner divisions and offices in order to maintain the highest achievable levels of protection of all data resources and reduce the overall threats to critical computer, technology and communications services.

As security headquarters, we provide information technology security services and timely advice to our client agencies. We act as diplomats to promote and maintain high levels of security consciousness throughout Michigan government. When circumstances require, we provide and assemble teams of specialists to respond to leading security issues or concerns.

Most importantly, we work diligently to keep Michigan's enterprise and agency networks, communications systems, computers, data and technology resources safe and secure from all known and predictable threats in an environment promoting ease of access and use.

OES combines our efforts with those of counterparts within MDIT and agencies across state government to instill and maintain the confidence and trust of staff, client agencies and citizens. Whenever opportunities exist, we act to position Michigan as a

Collaboration as the Centerpiece

Protecting Michigan's critical government information has become an ongoing, global challenge. The reality of today's cyber threats is that attacks against our critical infrastructure do not require physical access to targets to inflict great harm. In fact, persons bent on destruction could potentially carry out harmful attacks from the comfort of their homes—anonymously and thousands of miles away.

In order to provide the privacy and security that citizens rightfully expect, MDIT has established public and private sector partnerships to assist us in achieving ongoing protections. These local and national partners help us ensure the continued availability of e-government services in a safe, secure manner. Virtually every function of Michigan government relies on our reliable network infrastructure, whether working with local governments in local communities or communicating with federal partners.

As we move forward in the implementation of this strategic security plan, partnerships will continue to grow and develop added value. Some examples of key partnerships:

- Multi-State Information Sharing & Analysis Center (MS-ISAC): Working with our counterparts in the other 49 states and Washington, D.C., this organization provides real-time information on threats, vulnerabilities and remediation strategies to cyber incidents. The US-CERT Web site provides a wealth of information regarding cyber security from a variety of perspectives.
- Michigan Information Sharing & Analysis Center (MI-ISAC): Established in November 2006, this new organization is led by the Office of Enterprise Security and the Michigan chief information security officer (CISO). Rolling out the benefits of the MS-ISAC to Michigan local governments, this two-way communication provides essential coordination for cyber emergencies and coordination during virus attacks and other serious cyber situations. We envision this group growing from approximately 30 members to several hundred members over the next several years – thus providing a valuable resource to local partners.
- National Association of State Chief Information Officers (NASCIO) Security & Privacy Committees: This group coordinates public policy and develops research documents in coordination with states and the federal government.
- Federal Department of Homeland Security (DHS) committees & programs: NASCIO is represented on the Information Technology Government Coordinating Council (GCC) in Washington, D.C., by the Michigan CISO. Through jointly developing documents like the National Infrastructure Protection Plan's IT Sector Plan, a roadmap has been established to protect our nation's critical infrastructure in all sectors – including cyber. This document provides an essential list of future activities and this relationship continues to lead to new grants, programs and opportunities to protect Michigan families.
- Michigan InfraGard: A close-working relationship with the private sector is essential to improving the state's ongoing cyber security efforts. During 2004-2006, MDIT staff has participated in many InfraGard programs, conferences and outreach to schools. Additional activities are planned in the coming years.
- Universities, K-12 Education & Other Non-Profit Groups: We work with these groups to improve education and cyber ethics across Michigan.
- Pandemic Influenza Coordinating Committee (PICC): MDIT is actively involved in all aspects of Michigan's Pandemic Influenza Coordinating Committee (PICC). Working with public and private sector partners around the state and country, this committee is outlining technology's vital role in planning for affected emergency areas such as: transportation/ border, human health, animal health, public safety and individual/family/community.
- We are also addressing many new emergency management questions such as the need for telework during a pandemic emergency (www.michigan.gov/flu).

The Six's A's of Security

The six A's of Security are the lens through which we view processes, procedures, policies and services.

Administration: Development and publication of security policies, standards, procedures and guidelines, screening of personnel, security awareness training, monitoring of system activity and change control procedures.

Authentication: The process of identifying a subject or object, which can be checked and verified. It is usually differentiated between the authenticity of a message or file and the integrity of a transaction.

Audit: An independent examination of a work product or set of work products to assess compliance with specifications, standards, contractual agreements, integrity or other criteria.

Access Control: Protection of system resources against unauthorized access; a process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities.

Assessment: The method of identification of risks and assessing possible damage that could be caused in order to identify appropriate security safeguards.

Authorization: The process of determining what types of activities are permitted. Usually, authorization is in the context of authentication. Once you have authenticated a user, the user may be authorized different types of access or activity.

Michigan Cyber Security

www.michigan.gov/cybersecurity

In order to continue educating the public regarding cyber threats, identity theft, and a host of other Internet problems, we have developed an award-winning Web site on cyber security.

The site is constantly updated and improved to provide relevant facts, figures, training and related information to protect all Michigan citizens. Whether individuals, businesses, schools or families go online, we want them to be safe.

Enterprise Information Security Framework

Protecting citizen information is a priority for Michigan and its 19 executive branch agencies. The enterprise information security approach is a cross-agency solution geared toward establishing a formal statewide framework for information security in Michigan.

Through this framework, we are developing policies, standards and procedures for agency use. With these guiding principles in hand, agencies are empowered to map out their own course of implementation in cooperation with MDIT. The results unify the security approach for state employees and business partners.

This statewide framing of security affords agencies the ability to effectively conduct day-to-day business, while allowing the state to expand business functionality in a safe and secure way.

There are a wide variety of security needs and services provided by state agencies. These needs and services must be handled while maintaining legal and regulatory compliance and protecting the state's information assets from deliberate loss or misuse. Mechanisms to allow agencies to transmit data securely across networks and store data securely while protecting citizen information are paramount.

Guiding this process is the fact that information is neither confined to computer systems nor to an electronic or machine-readable form. MDIT has long-recognized that security must apply to all aspects of safeguarding and protecting information or data, in many forms. Therefore, protecting this information, along with the processing and delivery capabilities of this information, is considered a key state asset.

Central to this framework is also the adoption of Control Objectives for Information and related Technology (CoBIT) concepts and National Institute of Standards and Technology (NIST) best practices. These objectives and best practices will complement agency internal policies, standards and procedures and provide agencies the ability to protect the state's sensitive information to the fullest extent possible. This enterprise approach to information security allows the state and its agencies to act in a highly coordinated and efficient manner.

Goals and Objectives

Our goal is to equip agencies so that they can effectively utilize:

- Mechanisms that protect the reputation of the state and allow the state to satisfy its legal and ethical responsibilities to protect sensitive information
- A statewide approach to information security
- Methods that make policies, standards and procedures easy to understand and access based on roles with the organization
- Mechanisms that help identify and prevent the compromise and the misuse of the state's data, applications, networks and computers

The first, and most important, underlying objective of the enterprise information security approach is the development of policies, standards and procedures to identify the state's security requirements. This will assist agencies in implementing the appropriate controls to protect sensitive information for which they are responsible.

Initiatives

The initiatives to be undertaken in this process are as follows:

- Developing statewide information technology policies (Ongoing): Currently, MDIT, with state agencies, is rewriting existing and developing new statewide information technology policies to address the state's management view on what will be secured and who will be responsible for securing it through the use of management, technical and operational controls.

- Next, standards will be developed to address, on a more granular level, how the management, technical and operational controls are to be implemented and what the expected outcome of any action should be.
- Developing statewide information technology procedures (Ongoing).
- Finally, procedures will be developed with detailed step-by-step instructions on how the standards are to be attained to reach the goals.

This enterprise information security approach supports the strategic view of the state and helps build its security foundation of protection, while the information technology policies, standards and procedures formulate a security framework of protection.

Enterprise Information Technology Framework			
Security Awareness Policy	Access Control Policy	Information Security Policy	Aditional Policies
• Acceptable Use • Security Awareness Training	• Authentication & Authorization • Separation of Duties • User Account Management	• Data Classification Encryption • Media Disposal & Sanitation • Incident Response	Complete listing at: connect.michigan.gov/MDIT
Standards			
Procedures			
Guidelines			

Agency Security Plan Development

This project synchronizes the state of Michigan's efforts to assist agencies with the creation of standardized, unified, but department-specific, security plans. The primary tool to be developed for use in this endeavor is the security plan template. It will include the recommended documentation and categories to assist an agency with identifying what information is required, data gathering, problem area identification, prioritization of next steps and the interfaces to other strategic security initiatives.

The agency security plan will identify all information technology assets within the agency, the risks to each of these assets and how much time, effort and money the agency needs to expend to thoroughly protect these assets.

The Office of Enterprise Security will be responsible for the creation of the security plan template. As the agency security plans are created they will be incorporated into an enterprise master security plan document held by Office of Enterprise Security.

Goals and Objectives

As this plan moves forward, it will be guided by the following goals and objectives:

- **Create standard, comprehensive security plans across all state agencies**
  To accomplish this goal, a standardized template will be created for use across all agencies. It will serve as a tool for documentation and analysis of the agency's current overall security status. In order to promote the use of best practices from NIST, CoBIT and the Center for Internet Security (CIS), those standards will be incorporated into the template.
- **Coordinate business-side & MDIT business continuity/disaster recovery plans**
  The focus here is to assess business-side plans for business priorities and requirements and how they would interface with MDIT disaster recovery plans to facilitate a coordinated effort for minimal customer service interruption.

- **Enhance security awareness**
  We are working to promote additional programs for employee security training and awareness. This training will include ongoing, general user security awareness, as well as specific training on application security.
- **Security roles & responsibilities**
  Initiatives are underway to further define roles and responsibilities for Office of Enterprise Security liaisons and agency-side security and privacy officers and how each interfaces.

Project Outcomes

The desired outcome of this project is to unify state efforts in protecting Michigan citizens, to deliver the most effective approach possible. This will be accomplished through the development of a statewide security plan. Though the security plan will not create many of the programs necessary for a comprehensive security framework, it will document any existing programs, centrally gathering that information, while identifying those areas still in need of a complete security framework and how MDIT and its Office of Enterprise Security interface with these needs.

As described above, this security plan template and resulting plans will benefit from the direction of NIST, CoBIT and other national standards for best practices. Most importantly, it will be altered to fit the specific needs in protecting state of Michigan needs and assets.

Privacy Project

The state of Michigan has a broad responsibility for the social and legal environment in which private and sensitive information exists. The privacy project—outlined here—is for the state's executive branch, but every part of state government and most citizens have a stake in it. The state focus is on protecting private information related to both citizens and state employees. A critical piece in the success of this effort will be educating and equipping individuals to understand and implement it.

The scope of this project is to create a privacy approach that will define and create appropriate protection for the personal information collected or maintained by the state of Michigan. The state's executive agencies will depend on the outcomes of this project to guard against loss, unauthorized access and illegal use or disclosure.

While many of these efforts are already in place across Michigan's state government, this plan will formalize things in a specific and thoughtful way. The following goals and objectives are guiding the privacy project's development.

Goals and Objectives

In this section, we outline the goals and objectives related to developing a formal privacy approach for Michigan's executive branch:

- **Enhance agency-level accountability**
  Each agency must be responsible for managing personal information under its control as well as the assignment of responsibilities to their staff.
- **Improve notice information**
  Each agency must identify what personal information is gathered and the purpose for usage of that information. Whenever possible, a notice with this information should be given to the individual.
- **Improve consent procedures**
  If at all possible, consent should be obtained before data collection, storage and use. Sensitive information should always be gathered with explicit consent of the individual.
- **Minimize information collection**
  Agencies must only gather information necessary for purposes in support of their department.

- Reduce information retained
  Information should only be retained as required, and must include a set of guidelines for removal. Only the media approved by the agency may be used.
- Improve accuracy
- Meet or exceed privacy regulations
  Appropriate controls must be in place to meet or exceed state and federal privacy regulations or laws.
- Make disclosure more readily accessible
  The privacy policies and procedures should be readily available for public review when required. The policies must be updated when needed and communicated to internal personnel at least annually.
- Increase information access
  Upon request, access by an individual to their personal, private information may be allowed. The agency should also provide the individuals the ability to address inaccuracies.
- Facilitate challenges
  An individual may have the right to challenge an agency's compliance with the principles outlined in the goal section above. A venue must be in place for these challenges to take place.

Initiatives and Timelines

Provided here are the specific initiatives the State is undertaking in order to move this project forward (more details are available in Cyber Security-Appendix B):

- Privacy officer installation (FY 2008)
  MDIT will work with agencies to establish the privacy officer roles and responsibilities.
- State of Michigan privacy office creation (FY 2008)
  In an effort to create a state of Michigan privacy office, we will begin by defining the requirements and then assist with the establishment of it.
- Guideline development & dissemination (FY 2008)
  Guidelines are needed for the agency's privacy policy and procedures. MDIT will work to develop the guidelines and make agencies aware of them.
- Privacy office policy & procedure development
  MDIT will provide guidelines for the privacy office's policy and procedures.
- Data identification & documentation (FY 2009)
  It is necessary for the agencies and MDIT to identify and document where all state of Michigan privacy data are collected, used, displayed and retained.
- Privacy policy compliance process (FY 2009)
  To ensure compliance of privacy policies, MDIT and the agencies will create and implement an agreed-upon process.
- Privacy data electronic management (Ongoing starting in FY 2010)
  The responsibility for the initiatives related to this privacy framework development and implementation falls within three areas of state government: 1) the parent agencies where the data are needed to perform duties as assigned by state or federal laws or regulations; 2) MDIT as custodian of the electronic data; and 3) a new public-facing privacy group referred to in this plan as the state of Michigan privacy office.

Risk Reduction

In today's environment, there are numerous threats to the confidentiality, integrity, and availability of state information technology (IT) systems and the data that reside on them. Some of the risks to the state are from ever-changing threats, such as a well-worded phishing scam, while others are from insecure practices that have now become a part of our culture.

The strategies/initiatives that MDIT's Office of Enterprise Security (OES) is undertaking and that are described in this document are intended to reduce the state of Michigan's exposure to IT security risks. They include solutions that ensure systems connecting to the state's network are properly configured, that ensure vulnerabilities are being identified and remediated in an efficient manner and that minimize the potential impact of a security compromise.

A critical piece of this endeavor is assisting state agencies with the development of their own security plans. More details are provided in Cyber Security-Appendix A.

The initiatives we are undertaking follow industry best practices, address security issues identified by independent third parties and auditors and assist in complying with Payment Card Industry (PCI) standards and other state and federal requirements. The discussion includes the implementation of an endpoint security solution, a vulnerability management solution and several other risk-reducing strategies.

Goals and Objectives

- Raise confidentiality, integrity & availability
  In working to ensure that IT systems do not compromise the confidentiality, integrity or availability of state resources and data, specific objectives we are working to ensure systems connecting to state resources are configured in a secure manner and are not compromised thus allowing unauthorized access to state resources. We are also working to secure state-managed systems connected to non-state resources.
- Lower vulnerability
  As we work to identify and remediate system vulnerabilities in a consistent and efficient manner, we will develop processes and procedures to identify and remediate vulnerabilities in a consistent manner, acquire appropriate tools to identify vulnerabilities, integrate vulnerability remediation into MDIT culture and improve compliance with industry requirements/standards.
- Reduce risk
  When it comes to reducing the IT security risk to state IT resources, we will work to reduce presence of IT systems in the demilitarized zone (DMZ), a "neutral zone" between the private network and the public network, and better manage communications to and from state IT resources.
- Improve response time
  In this area, we will work to ensure our ability to identify and respond to IT security incidents in a timely and efficient manner.

Initiatives and Timelines

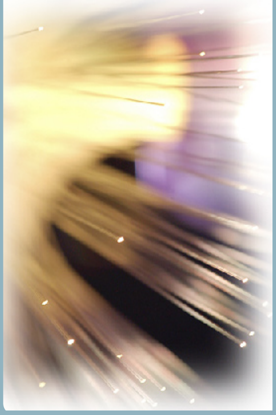
Provided here are the specific initiatives the State is undertaking in order to move this effort forward (more details are available in Cyber Security-Appendix C):

- Endpoint security and network access control (FY 2009)
  This initiative implements an endpoint security solution to ensure that systems connecting directly and remotely to the state's systems are secured appropriately. This will limit the devices which connect to the state's network to those that are confirmed to be running current anti-virus protection and are correctly patched against known vulnerabilities, protecting the state's information resources. Steps to implement these strategies have already begun.

- Formal vulnerability management program (FY 2008)
  This project will identify and remediate system vulnerabilities, including IT systems in the state's public-facing systems, servers on the network and state-managed systems connecting to the state's resources. MDIT's vulnerability management program will further ensure compliance with Payment Card Industry (PCI), state and federal standards for third-party vulnerability assessments and enhance the state's growing e-services to citizens and businesses.
- Critical information security upgrade (CISU) (FY 2008 & FY 2009)
  This is partnership between security and telecom teams is providing greater protection of vital files and data and keeping critical systems available to qualified users. Through 24 initiatives, more stringent safeguards against malicious/unauthorized traffic, and enterprise hardware/software system reconfiguration and upgrades are in motion. In the short term, additional firewalls will be installed to allow for greater flexibility in keeping applications available in the event of a virus outbreak. Also, vendor extranet hardening will occur to assist in keeping vendors from cross infecting each other in the event of a virus outbreak. In the next six months, network perimeter firewall upgrades will take place to allow for more capacity in dealing with increased traffic load due to potential virus activity. Within the next nine months, a project on firewall access control and intrusion prevention will be implemented to allow for greater flexibility in keeping critical systems available in the event of a virus outbreak. Also, Internet traffic blocking will occur; filtering a large subset of traffic types to the Internet that typically are used for malicious activity.

Risk Reduction: Initiatives and Timelines

- **Management of state network communications (FY 2009)**
  Limiting unnecessary communication and traffic from the state's Intranet to the public Internet will lessen exposure to potential threats. This initiative seeks to restrict that communication and reduce the spread of viruses via e-mail gateway filters and preventing infected systems from phoning home to be remotely controlled. Implementation of this initiative has already begun.
- **Policy/standard management and enforcement (Ongoing)**
  This initiative will identify and update legacy security policies and standards to ensure consistency and enforceability more effectively. Organizational and technological changes make it necessary to redefine and communicate existing policies in order to maintain cohesive operations and uniform standards across the enterprise.
- **Off-hours security monitoring and response (FY 2008)**
  Security and support issues can happen at any time and this initiative will establish a plan for providing evening and weekend coverage to support enterprise security functions. Off-hours monitoring and response will enable staff to identify and respond to threats more quickly and efficiently, thus preventing more serious compromise to the state's network.



Business Continuity: Disaster Recovery

A central piece of the MDIT mission is to implement plans and procedures by which state business and IT services may continue in the face of major disasters as well as during acts of terrorism, natural disasters and other emergencies. These efforts are collectively referred to as business continuity. In this section we discuss two categories of activity: disaster recovery and emergency management.

Disaster Recovery

MDIT is establishing processes and infrastructure to equip Michigan departments with the ability to recover any critical functions—no matter the extent of a natural or unnatural disaster—within 24 hours. The 2006 IT strategic plan identified Disaster Recovery (DR) as one of seven technology areas with potential to provide the state the greatest return.

Strategy in this area centers on the over 90 critical functions identified by the state agencies participating in the Continuity of Government Initiative (COGI), led by the Michigan Department of Management and Budget (DMB) and commissioned by the governor. The resulting Secure Michigan document identified disaster recovery as the number one priority for the state's IT program. In addition, disaster recovery requirements often must be met in order to obtain federal or state certification or implemented based upon laws, mandates, audits or guidelines.

Initiatives and Timelines

In the area of disaster recovery, MDIT will be working the following initiatives (more details are available in Cyber Security-Appendix D):

- Refresh the disaster recovery (DR) policy for the state of Michigan (FY 2009)
  It is imperative that the state first provide a clear direction and make a real commitment to implementing disaster recovery for its critical applications. MDIT will propose a policy that defines the level of disaster recovery for an application or technology asset based on business criticality and risk.

- Enhance organizational structure (FY 2008)
  MDIT is immediately considering assigning senior-level MDIT personnel to either a DR workgroup or committee. This group will drive decisions with input from the CIO and CISO.

- Execute a formal gap analysis study (FY 2008 & 2009)
  The gap analysis will require the input of the technical personnel assigned to specific critical and ancillary systems. Assessing interaction with other systems and the gap analysis may require MDIT and agency personnel to confer on redundancy, recovery time and inter-relational issues. Each year, 35 critical systems will undergo gap analysis on their DR level. Agency decision makers will benefit from this information as they determine requirements for implementation.

- Develop a technological needs list for data centers (FY 2008 & 2009)
  Each year, 15 of the 53 critical systems will be assessed. The resulting data will be utilized to illuminate shared component purchases. Based on the steering committee's input, outside contract integration experts may be called upon for assistance.

- Purchase a DR planning software technology (FY 2008)
  A DR planning software technology will be procured that contains functionality, including a granular level of update control; templates for different types of DR plans; compatibility with major software vendor call list applications and interface hooks to software. Use of the software should begin immediately after its purchase in 2008. However, configuring the software to the granular level of access that is needed throughout all of MDIT and the agencies will require one full-time employee.

- Integrate the DR planning software into the change management workflow (FY 2009-2010)
  Changes to any critical system's infrastructure requires a re-evaluation or gap analysis to determine if the recovery time objectives can still be met. The current change management workflow software should automatically notify the appropriate individuals of the need to reassess their piece of the DR plan. The gap analysis will identify necessary changes for action by the steering committee.
- Begin DR testing (FY 2009-2010)
  It will be important for us to test environments and make adjustments as we move forward. The testing should be phased in from modest level tests, to ensure no impact to the customer, to full failover tests that require customer use of the redundant system. Each group of individuals on the DR testing team will be obtained from the pool of technical staff assigned to the various critical systems.

Business Continuity: Emergency Management

We are aligning our emergency management approach with Michigan's overall information technology strategic plan ,as well as Governor Granholm's Hometown Security vision to "protect our citizens and make Michigan's communities safer." This vision recognizes the benefits of a fully-engaged, prepared, trained and well-equipped state agency.

Focused on minimizing the effects from acts of terrorism and natural disasters and other emergencies, we are embracing a department-wide approach and perspective to all planning and response activities, acknowledging that no individual group stands alone.

Emergency management is a dynamic process that includes planning, training, conducting disaster exercises, testing equipment and coordinating activities. The primary goal is to create and maintain an effective organization to mitigate, prepare for, respond to and recover from major threats to lives, livelihoods and property.

Goals and Objectives

- Formalize MDIT's emergency management planning, response and recovery
  We are developing written policies and procedures, an emergency management plan, an emergency operations planning process and are also working to operate and manage the Emergency Coordination Center and train staff.
- Protect critical Infrastructures
  Critical infrastructures are the complex systems that provide the services essential in our lives. They are currently organized into 17 sectors. Critical infrastructure protection (CIP) is a priority for the federal government, the private sector and state, local and tribal governments. MDIT, through OES, has been an active member of the state's CIP Board since its inception.

Initiatives and Timeline

- Policies and procedure development (FY 2008)
  Develop and implement an emergency management and operation plan policy and procedure.
- Formalize emergency management plan (Ongoing)
  Document the emergency management response organization, the responsibilities of the response organization, define the concept of operation and define the development and maintenance of the plan.
- MDIT emergency operations planning (FY 2008)
  Establish a MDIT emergency operations planning group, require development of emergency operation plans from MDIT groups, provide support to MDIT organizations in the development of emergency operations plans and develop exercises internal to MDIT to test the plan.
- Emergency Coordination Center operations & management update (FY 2008)
  Develop and document ECC procedures and develop an ECC located away from major attack centers such as downtown Lansing or the data centers.

- Emergency management plan training (FY 2008)
  Develop plan overview, an operational plan training and an emergency training for ECC Members, then provide training to MDIT staff to understand, deter, and interdict.
- Cyber attack mitigation (Ongoing)
  In this area, we are working to further mitigate cyber attacks against MDIT's critical infrastructure. We will update and refine standards/procedures, refine and establish processes and procedures to capture relevant information security risks, disseminate information throughout MDIT and develop metrics to support resource requests.
- Homeland Security relationship enhancement (Ongoing)
  We will continue as an active member in the state's critical infrastructure protection committee, participating and partnering with MSP's Emergency Management Division, participating in MSP-sponsored exercises and maintaining the MDIT Annex to the Emergency Management Plan.
- Other collaborative relationship enhancement (Ongoing)
  We will also continue collaborative relationships with various government and private entities to mitigate cyber attacks and information security risks. Organizations include: Multi-State Information Sharing and Analysis Center (MS-ISAC), InfraGard and NASCIO.
- State-local information sharing enhancement (Ongoing)
  We will increase the exchange between the Michigan Information Sharing and Analysis Center (MI-ISAC) and local units of government, establishing relationships with local IT organizations for the dissemination of cyber security information, rolling out the Multi-State Information Sharing and Analysis Center (MS-ISAC) portal and establishing procedures for rolling it out.
- Homeland Security grant-funding methodology (FY 2008)
  In an effort to further maximize homeland security grant dollars, we will continue to develop and maintain a grant distribution methodology with agreed-upon priorities and criteria requiring that all projects support the plan, demonstrate long-term benefits to the state and have systems in place for these benefits. We will also develop a framework and methodology for evaluating grant expenditures and effectiveness.
- Cyber security awareness campaign (Ongoing)
  We will continue the development of MDIT's cyber security Web site to promote self-reliance and personal safety, and develop a MDIT awareness program.

Training and Culture

A fundamental assumption in enterprise security management is that plans alone are not effective unless they are supported by people and a process brought together by good management skills and a philosophy of partnership. It is important to remember that all groups within MDIT will respond to and be involved with implementation of this plan. There must be concern, interest, support and participation by everyone within the department; this is not a one person job. Without full participation, there cannot be true success.

In order to protect state assets to the fullest extent possible, a multi-layered and highly extensible security architecture has been designed. This architecture seeks to utilize the absolute "best of breed" security products, devices and tools, combined with careful planning and policymaking, across the entire state of Michigan enterprise.

In addition to utilizing the best products and tools for each situation, an overall design/implementation strategy has been developed to further enhance the security of our data and resources. By utilizing risk analysis, security policy creation—including at the agency level (more on this in Cyber Security-Appendix A)—applications and data sources can be protected based on appropriate sensitivity levels.

According to this methodology, each e-government initiative data source or application is to be evaluated based upon its sensitivity, attractiveness to intruders and dependencies. Using this evaluation, the data source can be given a security rating that corresponds to a predefined level of protection that must be provided for that class of information. These different levels of protection will be constructed with the information at stake in mind. They will be composed of different combinations of security devices, tools and configurations designed to guard the data source from theft or attack in the most up-to-date and effective manner possible at all times.

Security Awareness

People, who are all fallible, are recognized as one of the weakest links in securing systems. The purpose of OES's security awareness training and education is to enhance security in Michigan by:

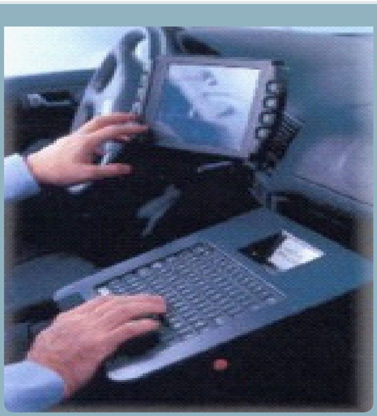
- Improving awareness of the need to protect system resources.
- Developing skills and knowledge so computer users can perform their jobs more securely.
- Building in-depth knowledge, as needed, to design, implement or operate security programs for organizations and systems.
- Educating users on the state of Michigan's Acceptable Use Policy and the signing of a state security agreement.
- Making state computer system users aware of their security responsibilities and teaching correct practices helps users change their behavior. It also supports individual accountability, which is one of the most important ways to improve computer security. Without knowing the necessary security measures and to how to use them, users cannot be truly accountable.
- Continuation of Homeland Security coordination by Michigan State Police.

The nervous system of Michigan's critical infrastructures are the hundreds if not thousands of interconnected computers, servers, routers, switches and fiber optic cables that make up state government's computer network. The healthy functioning of this network is essential to the overall health and welfare of Michigan's economy and security.

Michigan has been successful in using its computer network, along with the Internet, to increase commerce, community interaction and learning. However, at the same time, the use of the Internet has increased Michigan's risk of falling victim to Internet crime or cyber terrorism. Hackers, thieves and terrorists have adapted quickly to foil enhanced security mechanisms, finding new ways to steal personal and financial information. As a result, the need for increased security and security awareness is critical.

The federal government recognized and published the Computer Security Act of 1987 in response to Internet crime and cyber terrorism. This act requires periodic security awareness training for all federal employees involved in the management, use or operation of a computer system. Making staff aware of these threats has proven to be a very cost-effective countermeasure against security violations and/or mishaps. Gartner analysts Quellet, Proctor, and Witty (2006) estimated that there is a 0.8 probability of 25 % productivity savings in information security due to the workforce awareness of threats, risks and controls which reduces the number of security incidents. Staff that has been trained in a security awareness program will have the knowledge to prevent known incidents and/or mitigate the damage done when an incident does occur.

All of the work involved in creating a solid risk management and business continuity plan are worthless without a comprehensive awareness and training program for the individuals who are carrying out the plan. Therefore the development and implementation of a comprehensive training plan for everyone in MDIT—from employees to supervisors and functional managers to executive-level managers—is paramount.



Goals and Initiatives

Provided here are the specific initiatives the State is undertaking in order to move this effort forward (more details are available in Cyber Security-Appendix E):

Goal 1: Raise awareness

MDIT staff must understand the key elements and the necessity for information security as well as their personal role in security.

Initiative 1: Organizational policies & standards update

Initiative 2: Education/training enhancement

Initiative 3: Security awareness assessment

Initiative 4: Positive security behavior program development (FY 2007)

Goal 2: Enhance staff skills

We must educate and train staff on how to run systems most efficiently and how to develop and apply security controls.

Initiative 1: Key terms & concepts information program

Initiative 2: Categorical training program (FY 2008)

Goal 3: Improve over time

Practical and measurable outcomes are key for gauging our success and for retaining continued funding and support.

Initiative 1: Outcome tracking procedure development (FY 2008)

Initiative 2: Quarterly survey development (FY 2009)

Initiative 3: Online measurability campaign (FY 2009)

Initiative 4: Outcomes communication development (FY 2007)

Michigan's Enterprise Security Future

As part of Michigan's 2006 IT strategic planning process, MDIT and its clients—via the Michigan Information Technology Executive Council (MITEC)—examined technology and government business trends and their impacts. They reviewed both personal, professional observations and key worldwide trends as explained by industry experts, including Gartner and Forrester. The result of this exercise was the identification of technology solutions with the greatest ability to improve government services.

MITEC, in close collaboration with MDIT, chose specific technology solutions for further investigation of their possible enterprise-wide adoption. Since these technologies were selected, subcommittees comprised of representatives from MITEC and MDIT have reviewed where these technologies may apply to specific agency clusters and the state as a whole. The subcommittees prepared business case analyses of the most promising projects for each technology with the intent to integrate these technologies into the upcoming budget cycle recommendations for funding enterprise projects. One solution with the potential to provide the state with great benefit is mobile worker.

One Solution: The Mobile Worker

As noted in Michigan's IT strategic plan, the mobile worker initiative was designed around providing remote workers access to critical data, requiring adaptation and innovation. Technologies that support this trend include tablet PCs and laptops, Blackberry-like communications devices and wireless capabilities. The need for state employees to remotely access systems, services and data continues to increase. Advances in computer technology, the growth of wireless and digital products and the continuing expansion of the Internet are evidence that employees can work at any time and from almost any place.

According to research firm IDC, the global mobile workforce is expected to grow by more than 30 % by 2009. Given the shift to mobile working, business performance and productivity will soon depend on an organization's ability to understand, manage, control and secure tools and technologies that enable its mobile workers. Chief among these tools is remote access; connectivity to internal networks, applications and data from outside the office via mobile devices and wireless technologies.

In some parts of State government, the mobile worker concept has already been applied:

- Inspectors from the Bureau of Construction Codes are currently using rugged laptops on-site to perform inspections. Inspectors are able to log-in at home before coming to work in the morning to upload yesterday's inspections as well as download their current permits
- Michigan State Police officers have the capability to access various criminal justice computer systems from wireless laptops in their vehicles
- Unemployment Agency investigators are able to document their investigations while in the field and upload the changes to the main computer systems every night from home
- Department directors and key executives are piloting the use of Blackberry communication devices to improve productivity and be more accessible while away from their offices

MDIT will continue to evaluate wireless technologies and mobile devices and their associated risks to determine mitigation requirements and offer viable wireless and mobile solutions to our clients. The department also needs to ensure that agency executives are in a position to make informed decisions regarding the use of wireless technologies by their agency. This will assist agency staff in understanding the position taken by their respective department regarding wireless and what options have been approved and are available.

A comprehensive plan will be developed to address all aspects of deploying wireless technologies and mobile devices at the state of Michigan. Additional plans may be needed to address issues specific to the implementation and management of mobile and teleworker programs.

In addition to architecture, security, support and management issues, there is an identified need to actively manage user expectations regarding the use of wireless and mobile devices. The plan will include communications and planning components, with a focus toward arming state users with wireless security knowledge and awareness.

Existing services that support remote access to state resources—such as two-factor authentication with SecurID, VPN, dial-up—will be expanded to encompass any potential issues created by the introduction of wireless technologies.

MDIT will adapt policies, procedures and standards necessary to ensure that the state's wireless communications infrastructure/framework is deployed in an efficiently managed and secure way. Policies should allow for the education of users and define specific measures to increase awareness of wireless network security.

Wireless Technology Goals and Initiatives

In this area, our goals are focused around improving wireless service options, mitigating wireless technology risks and increasing wireless security knowledge and awareness among users. Specific initiatives that we are undertaking are as follows (more details are available in Cyber Security-Appendix F):

- Information security policy establishment (FY 2008) - An information system security policy addressing wireless technologies must be established.
- Change & control management process development (FY 2008) - Configuration/change control and management will ensure that equipment (such as access points) has the latest software release including security feature enhancements and vulnerability patches.
- Configuration standardization project (FY 2008) - Standardized configurations are needed to reflect the security policy, to ensure change of default values and to ensure consistency of operation.
- Staff training plan (FY 2008) - Security training to raise awareness about the threats and vulnerabilities inherent in the use of wireless technologies, including that robust cryptography is essential to protect the "radio" channel and that simple theft of equipment is a major concern.