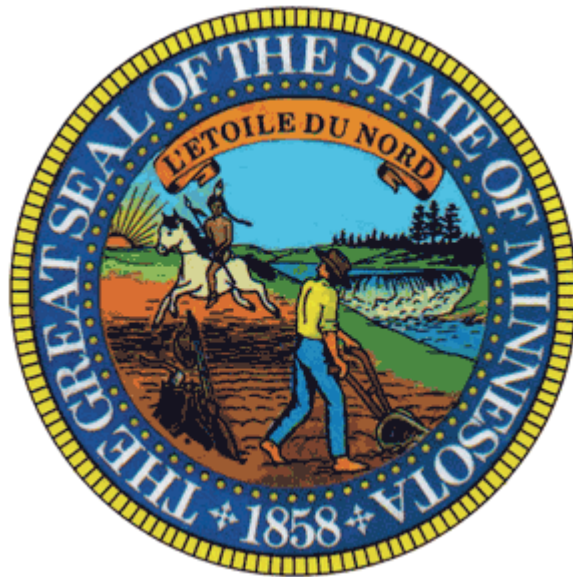


# State of Minnesota



## Enterprise Security Tactical Plan

**Fiscal Years 2010 – 2011**  
(July 1, 2009 to June 30, 2011)

*Prepared By:*

*State Chief Information Security Officer*

*The Information Security Council*



# State of Minnesota Enterprise Security Tactical Plan

## Contents

<b>Executive Summary</b> .....	<b>2</b>
<b>Introduction</b> .....	<b>3</b>
<b>Key Initiatives</b> .....	<b>4</b>
<b>Chapter 1: Legislative Mandate</b> .....	<b>5</b>
Initiative #1 – Legislative Funding Assessment .....	5
<b>Chapter 2: Improved Situational Awareness</b> .....	<b>6</b>
Initiative #2 – Security Information and Event Management .....	6
Initiative #3 – Security Intrusion Detection and Prevention .....	7
<b>Chapter 3: Proactive Risk Management</b> .....	<b>8</b>
Initiative #4 – Enterprise Vulnerability and Threat Management .....	8
Initiative #5 – Enterprise Security Program Framework .....	9
Initiative #6 – Information Risk Management Program .....	10
Initiative #7 – Security Awareness for Employees & Government Leaders .....	11
Initiative #8 – Identity and Access Management .....	12
Initiative #9 – Office of Enterprise Technology Security Program .....	13
<b>Chapter 4: Robust Crisis and Security Incident Management</b> .....	<b>14</b>
Initiative #10 – Enterprise Business Continuity Program.....	14
Initiative #11 – Enterprise Security Incident Management.....	15



## Executive Summary

The Information Security Council (ISC) and State Chief Information Security Officer are pleased to present the first Enterprise Security Tactical Plan for the State of Minnesota. This two-year plan prioritizes the tactical initiatives for the management, control, and protection of information assets. It also will help achieve the three strategic principles in the Enterprise Security Strategic Plan:

- **Improved situational awareness**, which includes continuous system monitoring and assessment of controls;
- **Proactive risk management**, such as solidly articulated requirements and ongoing security training; and
- **Robust crisis and security incident management**, which allows critical services to continue uninterrupted in a crisis.

The priorities and scope of the tactical initiatives in this plan could change over time. For example, due to reductions in Enterprise Security Program funding, the ISC has scaled back the scope of a Security Incident and Event Management initiative, started in fiscal year 2009. Conversely, the scope of other security initiatives have been expanded in response to the planned statewide data center consolidation and other Minnesota iGov planning efforts.

It is important to note that this plan does not cover the full breadth of security work being done by state agencies or the Information Security Council. Though not depicted in this plan, many operational activities happen each day that are vital to the security of the State.



## Introduction

With help from the Information Security Council, the Chief Information Security Officer worked to create the following mission for the Enterprise Security Program:

*“The Enterprise Security Program exists to support the efficient delivery of services to government entities and their customers; through a sustainable information security program.*

*The program will accomplish its mission through enterprise information security policies, standards, guidelines, and services that protect the state’s information assets and the security interests of the users of state services.”*

This plan outlines the tactical initiatives the State of Minnesota is undertaking over the next two years. These initiatives align with the following ten priorities identified in the Enterprise Security Strategic Plan:

- All state computer systems are continuously monitored for adverse information security events
- Government leaders at the highest levels understand and support the information security program
- All state employees receive ongoing security training appropriate to their job duties
- Information security program requirements are clearly articulated in a framework of policies, procedures, and standards
- Exploitable technical vulnerabilities in state computer systems are promptly identified and remediated
- People and entities that conduct business with state government have appropriate and timely access to the necessary computer resources and data
- State computer resources and data are protected from being used or accessed inappropriately
- The Office of Enterprise Technology serves as a leader by setting high standards for excellence in information security
- When information security incidents occur, government entities promptly contain, remediate, and manage those incidents
- Mission-critical services will continue in the event of a crisis



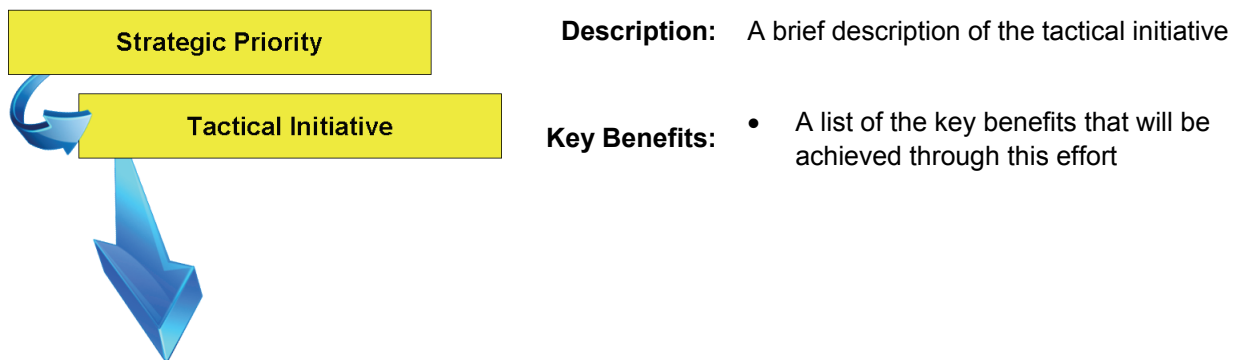
## Key Initiatives

The Enterprise Security Tactical Plan refers to high priority security activities as “**key initiatives.**” In some cases, active projects are already underway for key initiatives, while others are in the planning stage.

It is important to understand that this plan is not a complete inventory of work being done by the Information Security Council or state agency security professionals. Many day-to-day operational duties, such as assisting with the secure development of new government computer systems, are not in this plan.

Each key initiative has a narrative that describes why it is a high priority and the anticipated security benefits. This plan also outlines milestones for each key initiative, with anticipated dates for the achievement of those milestones. Finally, as illustrated in Figure 1, the plan includes a graphical depiction of how each key initiative links to outcomes the Enterprise Security Strategic Plan.

**Figure 1**  
**Linking Key Initiatives to Strategic Priorities**



### Key Milestones

Milestone Descriptions	Projected Due Date
Milestone #1	
Milestone #2	
Milestone #3	



## Chapter 1: Legislative Mandate

The 86th Legislature instructed the Office of Enterprise Technology and the Minnesota Management and Budget to develop a comprehensive funding strategy for enterprise security activities in the State of Minnesota. Chapter 101, Article 1, Section 10 included the following mandate in the appropriation laws for the Enterprise Security Program:

*“The chief information officer, in consultation with the commissioner of finance, shall develop a cost recovery plan for the 2012-2013 biennium to bill certain state agencies, constitutional officers, and other state and local government entities for the cost of information technology security. By March 15, 2010, the chief information officer shall report the plan and the potential for rates to be charged to agencies to the chairs and ranking minority members of the legislative committee divisions with jurisdiction over the budget for the office.”*

### Initiative #1 – Legislative Funding Assessment

This key initiative will help determine how the Enterprise Security Program can be sustained and made financially viable for the future. With assistance from agency partners and advice from independent consultants, this study will outline what security work needs to be done to provide the State of Minnesota with a secure information technology infrastructure. In addition, the study will recommend the best approach to pay for these security services.

#### Key Milestones

Milestone Descriptions	Projected Due Date
Assessment scope and methodology outlined	09/2009
Cross-agency team established to conduct and oversee work	10/2009
Preliminary report draft completed	01/2010
Preliminary report reviewed and approved by governance team and State CIO	02/2010
Final report presented to policymakers	03/2010



## Chapter 2: Improved Situational Awareness

Initiatives in this category will help the state obtain a better understanding of its risk posture and promptly respond to adverse events. They also will give the state the ability to measure its risk posture with rigorous performance metrics.

### Initiative #2 – Security Information and Event Management

Security information and event management (SIEM) is a solution for aggregating, correlating, and analyzing security event data in real time. SIEM solutions help organizations identify and promptly respond to threats, demonstrate compliance with regulatory requirements, and perform sophisticated forensic activities.

This initiative will take advantage of extensive technology research done by the Information Security Council during the past year to proceed with a SIEM pilot. Along with deployment of a SIEM tool, this key initiative will include the development of robust management processes. Long-term, SIEM will be a utility service offered to all entities in the Executive branch.

The SIEM pilot will include all data centers managed by the Office of Enterprise Technology. However, certain agencies may partner with the Enterprise Security Office to expand the centrally managed solution to their data centers. If the State of Minnesota proceeds with data center consolidation, SIEM technology will help address the increased security monitoring needs.

All state computer systems are continuously monitored for adverse security events



**Description:** Define core requirements for enterprise-wide security monitoring, and implementation of these practices within OET.

- Key Benefits:**
- Improved ability to identify complex cyber attacks
  - Reduced time and cost to investigate security incidents
  - Consistent and robust monitoring of all agencies, including those with limited resources

#### Key Milestones

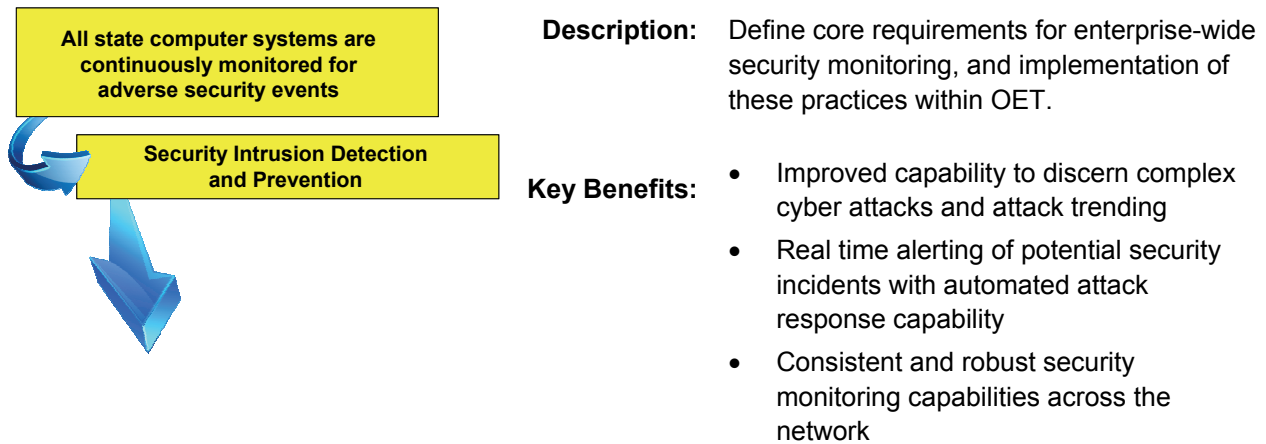
Milestone Descriptions	Projected Due Date
Improved situational awareness through SIEM implementation within OET	12/2009
Established baseline requirements for enterprise log management through a published standard	06/2010
Rollout of SIEM for agency systems supported by OET	12/2010
Established procedures for an enterprise SIEM solution	06/2011
Service-related documentation completed	06/2011
Strategic approach established for an enterprise SIEM integration with additional partner agencies	06/2011



### Initiative #3 – Security Intrusion Detection and Prevention

Intrusion detection and prevention (IDP) monitors and analyzes network traffic for potentially malicious security events. Through IDP solutions, security professionals can identify and promptly respond to threats, demonstrate compliance with regulatory requirements, and perform complex forensics. In very mature environments, IDP can be used to block malicious network traffic before it can cause harm. IDP is an important source of information for a robust SIEM solution, hence it is called out as a separate key initiative.

Security intrusion detection and prevention will eventually be offered as a utility service to all entities in the Executive branch. The implementation of the pilot IDP tools and the development of support processes has already started in the environments managed by the Office of Enterprise Technology. Expansion of the pilot implementation to other agency data centers is an important part of this key initiative.



#### Key Milestones

Milestone Descriptions	Projected Due Date
IDP sensor implemented at partner agency	09/2009
IDP service-related documents completed	12/2009
Baseline IDP architecture developed as part of design documentation	12/2009
Pilot IDP project expanded to include a partner agency	06/2010
Research completed on potential opportunities to partner with similar efforts ongoing at the federal government level	06/2010
Business case developed for enterprise-wide Intrusion Prevention System (IPS)	12/2010



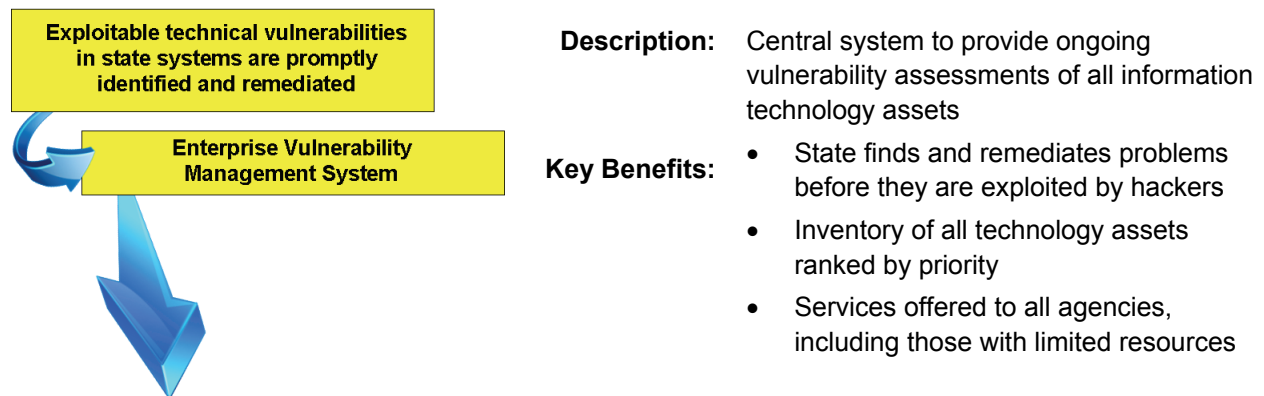
## Chapter 3: Proactive Risk Management

Initiatives in this category will make employees and government leaders more aware of security threats. They also will help garner the executive support needed for the Enterprise Security Program to thrive long-term. Finally, initiatives in this category include the implementation of preventive security controls, such as proactive vulnerability management.

### Initiative #4 – Enterprise Vulnerability and Threat Management

This key initiative provides a proactive approach to identify and mitigate security vulnerabilities before they can be exploited by hackers. Technologies in place today allow for the continuous assessment of the State’s information systems. These tools are augmented by the ongoing dissemination of threat and vulnerability information to all state agencies.

Implementation of the Enterprise Vulnerability Management System (EVMS) has been completed for almost all cabinet agencies. The next steps in this initiative expand the solution to the rest of the executive branch, primarily small and midsized agencies. This initiative includes milestones to build out standardized reporting as well as a central threat dissemination service. EVMS is an enterprise-wide utility service, and will continue to be so in the future.



#### Key Milestones

Milestone Descriptions	Projected Due Date
Enterprise Vulnerability Management Standard published	09/2009
EVMS installed in executive branch entities	12/2009
Full spectrum of reporting requirements defined	12/2009
Regular executive reporting standardized	06/2011
Threat Advisory process developed and operational	06/2011
Standardized scanning implemented across all executive branch entities	06/2011

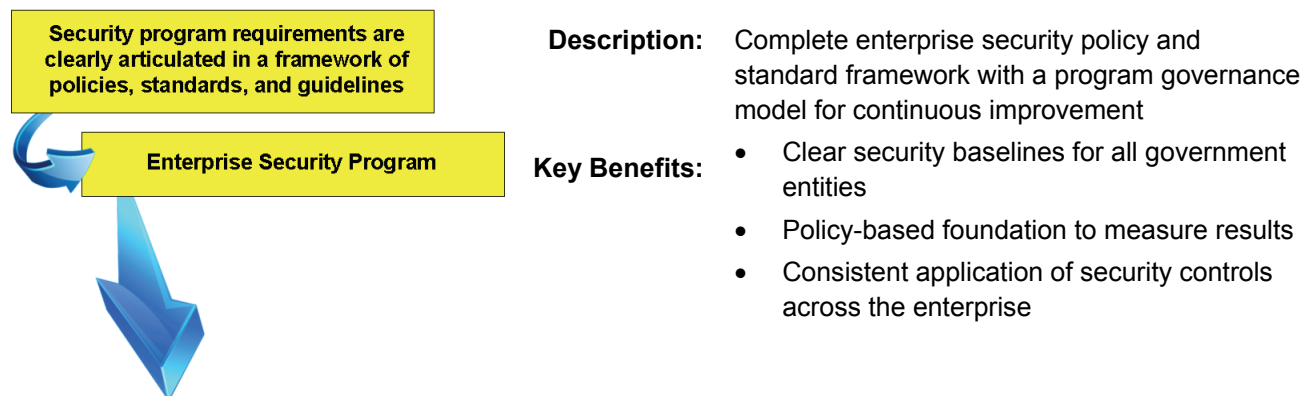


## Initiative #5 – Enterprise Security Program Framework

This key initiative establishes a policy-based foundation for the Enterprise Security Program. The Information Security Council made a decision to build the security program using a framework developed by the National Institute of Standards and Technology (NIST).

Over the past two years, the security community has worked to define, vet, and adopt a series of baseline security policies and standards, consistent with the NIST framework. These policies and standards flow through a collaborative governance process that includes agency Chief Information Officers, the Program Review Team, the Commissioners' Technology Advisory Board, and the State Chief Information Officer.

During the two years this plan covers, this initiative will result in the completion of the remaining baseline security policies and standards. Also, this initiative will yield a series of key performance metrics to measure and report on the State's risk posture.



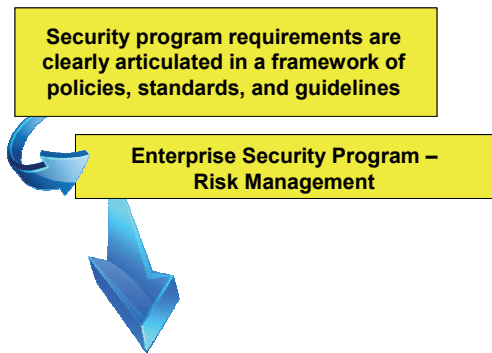
### Key Milestones

Milestone Description	Projected Due Date
Baseline enterprise security policy deck complete	12/2009
Exception process for enterprise policies and standards defined	12/2009
Baseline enterprise security standards complete	06/2010
Program performance indicator metrics identified	06/2010
End-user policy and standard training requirements defined	08/2010
Reporting on program performance metrics established	12/2010
Policy and standard maintenance program defined and operational	12/2010
Security architecture is integrated into the Enterprise Architecture	12/2011



## Initiative #6 – Information Risk Management Program

This initiative will define an enterprise risk management framework that will be used to identify security risks to the State’s information assets. This includes foundational processes to ensure that security controls are architected into new information systems from the onset. It also will ensure that residual risks are understood and accepted by management before systems are moved into production. Recognizing that risks change over time, a key outcome of this effort will be a process to continuously reassess security controls as information systems mature. And finally, to be useful, the Risk Management Program must provide ongoing and meaningful metrics to executives for informed decision making.



**Description:** Enterprise-wide risk management processes to enable better risk-based decisions by government entities’ leaders.

- Key Benefits:**
- Better understanding of the enterprise risk profile
  - Better understanding by government entities of their information security risks
  - Consistent delivery of security controls through security plans and security authorization

### Key Milestones:

Milestone Descriptions	Projected Due Date
Enterprise Security Risk Management, System Life Cycle Planning, and Security Authorization Guidelines published	10/2009
Enterprise Security Asset Criticality Standard published	11/2009
Enterprise Security Management Control Policies published <ul style="list-style-type: none"> <li>• Security Risk Management Policy</li> <li>• System Life Cycle Planning Policy</li> <li>• Security Authorization Policy</li> </ul>	02/2010
Enterprise Security Risk Assessment, System Life Cycle Planning, and Security Authorization Standards published	06/2010
Initial Enterprise Security Risk Gap Report published	12/2010
Enterprise risk posture continuously measured through a governance, risk, and compliance tool	06/2011

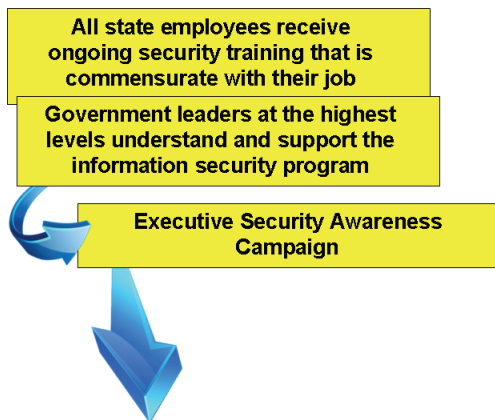


## Initiative #7 – Security Awareness for Employees & Government Leaders

Employees are often the weakest link in an organization’s security defenses. Therefore, it is important to educate employees so that they understand pertinent security risks and know what needs to be done to protect resources and data.

Current resource restraints will impede our ability to achieve all of our security awareness strategic goals. However, this initiative will make sure that the State of Minnesota makes significant progress during the current biennium. Milestones identified below will provide a minimal level of security awareness and create a baseline set of requirements for the future.

It is important to stress that the Information Security Council will continue to host critical security training to the extent that resources permit. For example, in fiscal year 2009 plans are already in place to train over 100 state agency information technology and security professionals through partnerships with the SANS Institute and the Minnesota State Colleges and Universities.



**Description:** Ongoing and comprehensive security awareness program for all state employees and government leaders / policymakers

- Key Benefits:**
- Better awareness of security threats capable of impacting government operations
  - Fewer security incidents caused by employee mistakes
  - Common baseline of knowledge for all employees
  - Clear understanding of all enterprise security initiatives
  - Support for the Enterprise Security Program

### Key Milestones

Milestone Descriptions	Projected Due Date
Annual State Cyber-Security Awareness Month campaign	10/2009 & 2010
Annual Government Leaders Security Retreat	10/2009 & 2010
Enterprise Security Awareness & Training Policy published	12/2009
Enterprise Security Awareness & Training Standard published	05/2010
SANS training events complete	03/2010
Enterprise Security Awareness Program initiated	06/2011



## Initiative #8 – Identity and Access Management

The first part of this initiative, Identity and Access Management Program, will help the state develop a common vision and common processes for controlling access to information resources. The starting point will be the creation of governance and technical committees. These committees will build on work done to date to develop, vet, and refine a comprehensive identity and access management strategy. Primary emphasis will on the creation of an identity structure for employees, business partners and citizens that can be used by all government entities. This initiative will also search for ways to streamline existing identity management operations to improve efficiency and promote consistent security practices.

The second part of this initiative, Access Control Services, will add more features, functionality, and customers to the identity and access management solution hosted by the Office of Enterprise Technology. This solution provides centralized authentication and authorization services for state government on a fee-for service basis.

People and entities that conduct business with state government have appropriate and timely access to the necessary information resources

State information resources are protected from being used or accessed inappropriately



**Description:** Centralized and streamlined access control solution for state government

- Key Benefits:**
- Better security through uniform and repeatable access control processes
  - Better experience for users of state services by providing all access through a single user ID and password
  - Reduced costs to develop new government systems by leveraging an external access control solution

### Key Milestones

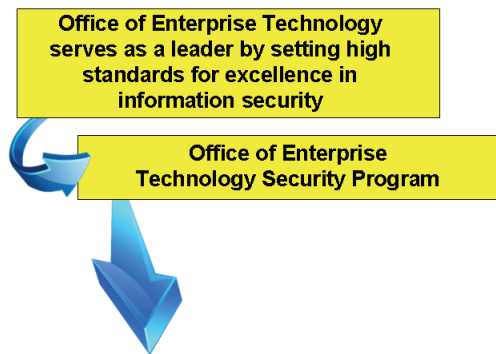
Milestone Descriptions	Projected Due Date
<b>Identity and Access Management Program</b>	
IAM steering and technical committees formed	10/2009
Risk and security requirements for statewide service developed	06/2010
Statewide single sign-on functionality developed	12/2010
Processes defined for integration and alignment with federal identity standards	03/2011
Comprehensive strategy and technical roadmap developed for enterprise service	06/2011
<b>Access Control Services</b>	
Integration with other statewide directories developed	09/2009
Log / audit reporting interfaces / distribution methods developed	10/2009
Enhanced identity and access management functionality developed	12/2009
Automated Integration with external log / reporting tools developed	03/2010
Plan for service migration to statewide solution developed	06/2010
Migration of service to statewide solution implemented	02/2011



## Initiative #9 – Office of Enterprise Technology Security Program

This initiative, started in fiscal year 2008, will enhance and mature Office of Enterprise Technology’s (OET) security to be a best-in-class information security program. OET must be a security center of excellence because it houses many critical government computer systems and sensitive data. The proposed data center consolidation effort will compound the need for extremely robust preventative, detective, and corrective security controls in the central technology agency.

Under this initiative, OET will serve as a leader by piloting new security technologies and developing robust processes that can be leveraged by all agencies. OET will also lead statewide efforts to define secure configuration standards for software and hardware products.



**Description:** Develop and institute a robust information security program to protect the confidentiality, availability and integrity of data and information systems assets managed by OET.

- Key Benefits:**
- Able to comply with the Enterprise Security Program and applicable business and regulatory requirements
  - Long term diligence in protecting data and systems entrusted to OET’s care
  - OET Information Security Program can serve as an example for agency security programs.

### Key Milestones

Milestone Descriptions	Projected Due Date
OET security awareness and training program plan completed	01/2010
Core security standards defined for critical software	06/2010
Security performance metrics reviewed regularly by agency leaders	06/2011



## Chapter 4: Robust Crisis and Security Incident Management

Initiatives in this category will help the State of Minnesota promptly respond to and manage security incidents to minimize damage. They also will help the state continue mission critical services in times of crisis.

### Initiative #10 – Enterprise Business Continuity Program

History has shown that even well managed services can become victims of catastrophic failure. The Enterprise Business Continuity Program helps mitigate these risks through detailed planning activities, including business impact analysis, recovery strategy development, business continuity planning, and disaster recovery exercises.

This ongoing initiative will facilitate the prioritization of services for the State as a whole and define appropriate recovery strategies for critical information systems. It also will help move the state closer to compliance with the enterprise policy and standard for continuity of operations.



**Description:** Ongoing continuity program to address unanticipated disruptions to government services

- Key Benefits:**
- Faster recovery of priority government services during a crisis
  - Reduced costs through leveraging shared recovery environment
  - Better ability to share staff during times of crisis through adoption of a common plan format, processes, and tools

#### Key Milestones

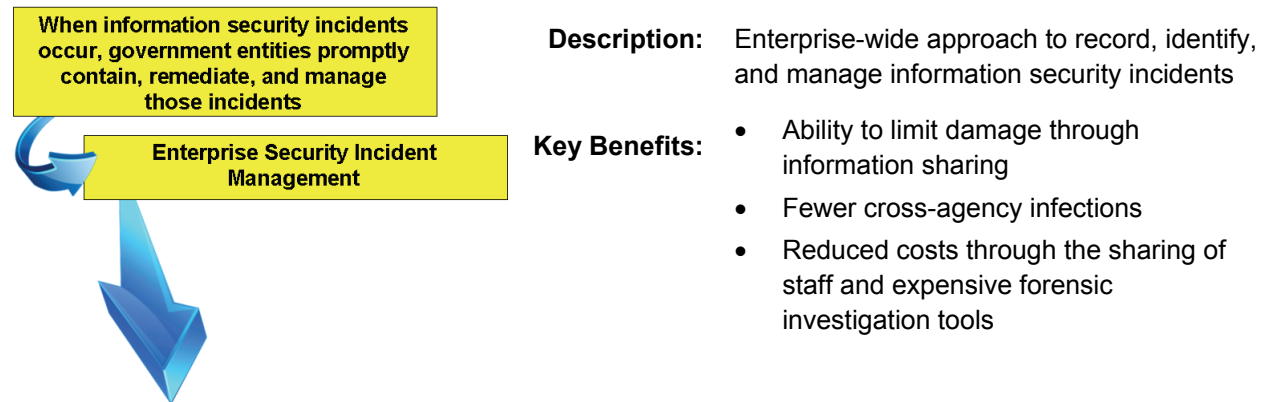
Milestone Descriptions	Projected Due Date
Agency pandemic plans in LDRPS	12/2009
COOP templates and policies in LDRPS	12/2009
Training for agency business continuity coordinators conducted	09/2010
Recovery strategies implemented	12/2010
State Recovery Center improved	12/2010
Continuity of operations plans completed	12/2010
Initial awareness training completed	06/2011
Enterprise compliance with COOP Policy and Standard	06/2011



### Initiative #11 – Enterprise Security Incident Management

Security incident management and computer forensics seek to determine the cause, scope, and impact of incidents. The goal of incident management is to stop unwanted activity, limit damage, and prevent recurrence.

The Enterprise Security Office and Information Security Council have worked to develop incident response and data forensic processes. This initiative will now work to install these processes in all executive branch agencies as a shared utility service. Adopting a collaborative approach will improve the State’s ability to identify and isolate incidents, thereby limiting damage.



#### Key Milestones:

Milestone Descriptions	Projected Due Date
Enterprise security incident management standard published	10/2009
Security incident management metrics developed	12/2009
Executive reports and reporting process developed	06/2010
Metric reporting tool selected and implemented	06/2011