

Montana Information Security Advisory Council
Purpose, Mission, Goals, and Objectives – 2015 Biennium
(Working Group Recommendation 9/3/15, 3:40pm)

Purpose

The purpose of the Montana Information Security Advisory Council (MT-ISAC) is to advise the Governor with respect to a statewide strategic information security program. (Governor Bullock executive order 05-2015)

Guiding Principles

- Citizen information privacy is paramount.
- Information security policies, processes, and laws will support and not hamper State of Montana businesses or government.
- Share appropriate information and best practices between public and private sectors.
- Unwarranted duplication will be minimized by sharing data, IT infrastructure, systems, processes, applications, and services where applicable.
- Flexibility: Some organizations have different security requirements and therefore security solutions should be tailored to address the level of risk present.

Mission

The mission of the State of Montana's Information Security Advisory Council (MT-ISAC) is to recommend an integrated interagency information security strategy to enhance the State information security posture.

The strategy includes the following goals that follow the NIST Security Framework of identify, protect, detect, respond, and recover and provides the foundation for the objectives below them. These objectives are for the current biennium and are recommendations to do the stated action. They have been designed to improve the state's situational awareness by developing a strong governance, posture, and response toward a current and future security strategy.

Goals/Objectives

1. **Identify** - Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
 - 1.1. Update State of Montana information security policies and documents to align with the **NIST** Cybersecurity Framework.
 - 1.2. Develop and implement a statewide standardized information security program **assessment** and measures for Departments and the State.
 - 1.2.1. Provide a yearly State information security assessment to the Governor showing program successes and a plan to address shortcomings.
 - 1.2.2. Develop a Governor's information security dashboard.
 - 1.3. Implement a statewide standardized **system risk management** template (measures, authority to operate, etc) based on best practices.

- 1.4. **Share** risk management guidance and recommendations with local governments and the private sector.
 - 1.5. Recommend new **legislation** or update current statutes, administrative and criminal, to address the present-day information security environment.
 - 1.6. Recommend **resources** (funding, people, etc.) and methods, such as Security Assistance Teams (SAT), to assist agencies in performing work in order to enhance the agency, and thereby the State, information security posture.
 - 1.7. Encourage development of a trained and educated information security workforce in Montana through the **University** System with private sector input.
 - 1.8. Assess an **apprenticeship** or internship program to develop hands-on information security skills.
 - 1.9. Identify **key players** within industry sectors and provide a forum for developing guidance and communicating with industry sectors.
 - 1.10. Collaborate with private industry to understand the information security posture of **critical infrastructure**.
2. **Protect** - Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- 2.1. Implement a comprehensive **information security awareness and training program**
 - 2.1.1. For managers, users, contracted support, and IT staff.
 - 2.1.2. Develop a campaign to deliver the message of information security in a positive and informational manner that engages the listener and encourages them to integrate information security into their daily activities.
 - 2.1.3. Support and participate in statewide information security groups and help to facilitate and leverage the existing communications channels.
 - 2.2. Enhance **situational awareness**.
 - 2.2.1. Document standing threat/vulnerability needs/sources and determine fast, efficient, and secure sharing methods.
 - 2.2.2. Foster better communication in information security between federal, state, local, and tribal governments.
 - 2.3. Collaborate with other States and organizations and utilize/leverage industry **best practices**.
 - 2.3.1. Evaluate the State of Washington's best practices and training of the cyber unit of the National Guard and apply similar practices in Montana where applicable (DOA, DOJ, National Guard, etc).
 - 2.4. Develop and implement process(es) for comprehensive **patch management**.
 - 2.5. Develop **limited user rights** strategy for state information systems.
 - 2.6. Identify **legacy systems** which exist on the State of Montana network and create a plan for securing or removing those systems.
 - 2.7. Recommend software, hardware, services, processes, and resources to increase **protection capabilities**.

- 2.8. Recommend security requirements for solicitation of and inclusion in state **contracts** involving information technology. Address breach language in contracts.
 - 2.9. Provide information on best practices for information security **insurance**, recommendations, (training) options, awareness, coverage, cost, and other considerations.
 - 2.10. Recommend methods and/or tools to inventory authorized and/or **unauthorized software**.
 - 2.11. Identify location of **sensitive data** and methods to protect it.
3. **Detect**- Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
 - 3.1. Recommend software, hardware, services, processes, resources, etc. to increase **detection capabilities**.
 4. **Response**- Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
 - 4.1. Recommend software, hardware, services, processes, and resources to enhance agency and State **incident response** - tools, procedures, checklists, lessons learned, and guidelines.
 - 4.2. Enhance State information security **law enforcement** capability.
 - 4.2.1. Improve the State of Montana's investigative expertise in the information security area.
 - 4.2.2. Explore additional resources in DOJ/DCI for Network Cyber Investigations.
 - 4.2.3. Research and recommend criminal investigative response in coordination with HSA, DOA, DOJ, and FBI.
 - 4.2.4. Develop a plan to increase the education of Montana's law enforcement group regarding information security.
 5. **Recover**- Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
 - 5.1. Recommend software, hardware, services, processes, and resources to enhance agency and State system **recovery** - tools, procedures, checklists, lessons learned, and guidelines.

MT-ISAC will refer to the National Institute of Standards and Technology (NIST) [Glossary of Key Information Security Terms](#) for a list of NIST definitions.