

July 15, 8:30 – 11:00
Room 152 – State Capitol

8:30–8:45	Call to Order, Overview of ISAC and Introductions	Ron Baldwin, Interim Chair
8:45–9:15	Operating Procedures (20 minutes) Board Discussion and Questions (10 minutes) Action Item	Lynne Pizzini
9:15–10:15 9:35	Goals and Objectives of ISAC (30 minutes) 10 minute break Board Discussion and Questions (15 minutes) Action Item	Lynne Pizzini/Joe Frohlich
10:15–10:35	Enterprise Security Policies (15 minutes) Board Discussion and Questions (5 minutes)	Joe Frohlich
10:35–10:55	Overview of Montana Analysis & Technical Information Center (15 minutes) Board Discussion and Questions (5 minutes)	Bryan Costigan
10:50–11:00	Open Forum <ul style="list-style-type: none"> • Future Agenda Items • Public comment 	Board Members Audience
11:00	Adjourn	Ron Baldwin, Interim Chair

Next Meeting: August 19, 2015

Notice: The Department of Administration will make reasonable accommodations for persons with disabilities who wish to participate in the ITB public meetings or need an alternative accessible format of this notice. If you require an accommodation, contact the Department of Administration no later than six business days prior to the meeting of interest, to advise us of the nature of the accommodation that you need. Please contact Joe Frohlich (406)444-3119 or email jfrohlich@mt.gov

Information Security Advisory Council Goals and Objectives – 2015 Biennium

Mission

The mission of the State of Montana's Information Security Advisory Council (ISAC) is to ensure that Montana's information systems are safe, secure, and resilient.

Three key concepts provide the foundation of this vision:

- Governance
- Posture
- Response

In turn, these key concepts will drive broad areas of activity that will define the ISAC objectives for the next two years. These goals and objectives define a framework to describe what it means to identify, prevent, protect, respond and recover, as well as incorporate security into Montana's information systems to ensure resilience.

Goals

- Advance Montana's overall security **Governance** by adopting a framework of standards and processes.
- Advance Montana's overall security **Posture** through proactive risk management, cyber workforce development, and industry best practices for cybersecurity.
- Advance Montana's overall security **Response** to the ever-changing cybersecurity landscape.

Objectives

- **Governance**
 - Establish through Executive Order an Information Security Advisory Council (ISAC) that includes state, local, National Guard, and private sector representation.
 - Implement an Enterprise Security Program in conjunction with the ISAC to ensure effective implementation of cybersecurity in all agencies of state government.
 - Develop an interagency information security strategy with initiatives, priorities, policies, standards, and roles and responsibilities to enhance the state cybersecurity posture.
 - Update State of Montana cybersecurity policies to align with the NIST Cybersecurity Framework.

- Begin the enterprise program by addressing gaps focusing on state government and expanding to the private sector over time through the use of the ISAC.
- Develop standard accountability processes for Department heads to ensure cybersecurity.
- Create a strategy to promote cybersecurity situational awareness for all users.
- Foster better communication in cybersecurity between federal, state, local, and tribal governments.
 - Formalize information sharing protocol and document standing information needs between HSA, DOA/SITSD/CISO, AND DOJ/DIC/MATIC.
- Understand the value of the University System's security needs
 - Document the University System perspective of their cybersecurity preparedness and the threats that they face, help develop a strategy of best practices, and assist with how to best promote cybersecurity.
- Encourage development of a trained and educated cybersecurity workforce in Montana through the University System with private sector input
 - Include an apprenticeship or internship program to develop hands-on cybersecurity skills.
- Understand the value of the Local Government security needs.
 - Document the Local Government perspective of their cybersecurity preparedness and the threats that they face, help develop a strategy of best practices, and assist with how to best promote cybersecurity.
- Understand the value of the Montana Local Business security needs.
 - Document the Local Business perspective of their cybersecurity preparedness and the threats that they face, help develop a strategy of best practices, and assist with how to best promote cybersecurity.
- Recommend new legislation or updates to existing laws such as reporting requirements to government and citizens as appropriate.
 - Create recommendations to update current state statutes, both administrative statutes for state government needs and criminal statutes to address the present-day cybersecurity environment.

➤ **Posture**

- Begin to assess security posture and readiness of each Department in state government.
- Develop strategy for better patch management
- Develop limited user rights strategy for state information systems.
- Identify legacy systems which exist on the State of Montana network and create a plan for securing or removing those systems.

- Develop a campaign to deliver the message of cybersecurity in a positive and informational manner that engages the listener and encourages them to integrate cybersecurity into his daily activities.
- Support a statewide cybersecurity training program to serve technical and managerial needs.
- Collaborate with private industry to understand the cybersecurity posture of critical infrastructure.
- Establish a communications procedure for receiving input from and sharing information with the public, state agencies, and local governments.
- Develop a Governor's cybersecurity dashboard
- Provide a yearly information security assessment to the Governor showing program successes and shortcomings with a plan to address shortcomings.
- Conduct internal evaluations of the statewide cybersecurity program.
- Explore training of DOA/DOJ/National Guard staff to defend against cyber-attacks through the use of the State of Washington National Guard cyber unit.
- Evaluate the State of Washington's best practices of the cyber unit of the National Guard and apply its practices in Montana where applicable.
- Recommend appropriate cost-effective safeguards to reduce, eliminate, or recover from identified threats to data.
- Develop a plan to increase the education of Montana's law enforcement group regarding cybersecurity.
- Advise on security requirements in the specifications for solicitation of state contracts for procuring information technology resources.
- Develop and implement a state Risk Management services program.

➤ **Response**

- Recommend resources (funding, people, etc.) and possible methods to obtain cybersecurity teams, in order to enhance the State information security posture.
- Move forward with state preparedness and migrate toward evaluation of the role with private sector as time and resources allow.
- Assess the feasibility of Security Assistance Teams (SAT). Teams may be comprised of security representatives from state agencies to help with risk assessments, make recommendations, write documents, and conduct training to help agencies be more secure based on ISAC direction and industry best practices.
- Research and recommend criminal investigative response in coordination with HSA, DOA, DOJ, and FBI.
- Explore additional resources in DOJ/DCI for Network Cyber Investigations.
- Improve the State of Montana's investigative expertise in the cybersecurity area.
- Provide technical and managerial assistance relating to cybersecurity.

Information Security Advisory Council (ISAC) Operating Procedures July 2015

OVERVIEW:

The State of Montana Information Security Advisory Council (ISAC) herein referred to as “Council” was established in 2015 by Executive Order NO. 05-2015 by Governor Steve Bullock. The Council serves at the pleasure of the Governor. The Council is advisory in nature as per MCA 2-15-102 Advisory capacity means “furnishing advice, gathering information, making recommendations, and performing other activities that may be necessary to comply with federal funding requirements and does not mean administering a program or function or setting policy.” The council consists of ten to fifteen members, representing the various State and Federal agencies, universities, and local governments that have an interest in cyber security. These members are to be appointed in March of each biennium. The ISAC will suggest to the Governor a slate of individuals as the Council members of the ISAC for the coming biennium. The Governor will appoint the Chair.

Responsibilities of the Council:

The purpose of the Council is to advise the Governor with respect to a statewide strategic information security program. The Council shall:

- Develop an interagency information security strategy with initiatives, priorities, policies, standards, and roles and responsibilities to enhance the State information security posture;
- Recommend resources (funding, people, etc.) and possible methods to obtain them, in order to enhance the State information security posture;
- Provide a yearly information security assessment to the Governor showing program successes and shortcomings with a plan to address shortcomings;
- Establish a communications procedure for receiving input from and sharing information with the public and the various agencies;
- Support a statewide security training program to serve technical and managerial needs;
- Advise on security requirements in the specifications for solicitation of state contracts for procuring information technology resources;
- Provide technical and managerial assistance relating to information technology security;
- Recommend appropriate cost-effective safeguards to reduce, eliminate, or recover from identified threats to data; and,
- Conduct internal evaluations of the statewide security program.

MEMBERSHIP & PARTICIPATION:

The Council requests an extension each biennium per §2-15-122, MCA. This request will include a recommend change in the Council membership. Each biennium in March, Council members and Security Representatives will nominate Council members that best represent the State in the area of cyber security. It is recommended that Council members have an interest and knowledge of cyber security topics. Each Council member will have to sign a confidentiality agreement to encourage open discussion in an event of a closed door meeting. The nominated list of members will be forwarded to the Governor's Office for review and approval for the coming biennium. The Governor will select a Chair. The Chair will get to select a vice Chair. The State CIO or their designee is automatically a member of the council.

VOTING:

Each Council member has one vote. It should be noted that given the advisory nature of the Council, votes indicate the degree of consensus, not an approval or denial of any item.

PARTICIPATION:

COUNCIL MEMBER PARTICIPATION:

Active participation is necessary for the Council to function effectively. Continuity is essential regarding issues under discussion, and especially for those needing affirmative action. Council members are strongly encouraged to attend meetings. A Council member may designate an alternate representative (with notification to Chair) to represent the member on occasions when the member cannot attend. The designated alternate may vote of behalf of the member. Should the Council as a whole feel that a Council member is not fully participating, the Council can, in consultation with the agency or institution's director, recommend replacement of the member in question.

SECURITY REPRESENTATIVE PARTICIPATION

CIO's/IT Managers/Security Officers of the State of Montana's State agencies, Local and Tribal Governments, universities, and private entities are encouraged to actively participate within the ISAC meetings and or workgroups.

STATE INFORMATION TECHNOLOGY SERVICES DIVISION (SITSD) PARTICIPATION:

It is anticipated that, upon request, portions of the general meetings will include presentations by members of the SITSD technical and policy staffs. SITSD will ensure that staff with technical knowledge of the issue(s) is available at council meetings to share expertise.

COMMUNICATIONS:

The Council shall communicate with SITSD, the Information Technology Board and other entities through the Chair, or as delegated by the Chair. Members are encouraged to contact the Chair with suggested agenda items. Items requiring Council action will be noted on the agenda.

Official correspondence will be distributed at the discretion of the Chair, or the Acting Chair, with the assistance of SITSD Council support staff. Action items or issues for future discussion will be noted by support staff, and coordinated with the Chair for future agendas.

Minutes of the Council meetings will be provided to all Council members and interested IT security professionals. They will be published on the SITSD web site.

MEETINGS:

The Council regular meetings are held on the third Wednesday of every month from 8:30AM until approximately 10:30AM. IT professionals from federal, state, local, and tribal governments, universities, and private entities are invited and encouraged to join in discussing security topics of interest. The Council reserves the right for closed door meetings under MCA 2-6-102 (4) should the need arise to address issues of high sensitive matters. Some information security information is identified as confidential and cannot be discussed in public meetings. The council would only utilize these types of meetings to discuss information that is classified as confidential.

STAFFING:

The SITSD provides staffing support to the Council. Such staffing consists of the Enterprise Security Program Manager and one individual providing administrative support. Council staffing support includes participating in building meeting agendas for monthly Council meetings, coordinating meeting times and rooms, taking minutes, distributing correspondence, and responding to the ad hoc needs of the Council. SITSD will also provide technical resources for assigned subcommittees as requested by the Council Chair.

EFFECTIVE:

These procedures will become effective upon approval at the July 2015 meeting. They will remain in effect commensurate with the Executive Order that establishes the Council.