

# Montana Information Security Advisory Council

## Meeting Minutes July 15, 2015

Attendees	
Meeting Chairperson: Ron Baldwin, State CIO	
Name	Affiliation
Erika Billiet	City of Kalispell
☪ Senator Mark Blasdel	(R) SD 4
Joe Chapman	Department of Justice
Bryan Costigan	MATIC/Department of Justice
John Daugherty	Department of Corrections
Sherri Davidoff	LMG Security
Maura Fleetwood	State Information Technology Services Division
Joe Frohlich	State Information Technology Services Division
Stuart Fuller	Department of Public Health & Human Services
Kreh Germaine	Department of Natural Resources & Conservation
Adrian Irish	The University of Montana
Margaret Kauska	Department of Revenue
☪ Representative Kelly McCarthy	(D) HD 49
Lynne Pizzini	State Information Technology Services Division
Major General Matthew Quinn	Director of Military Affairs, Montana National Guard
Manuel Soto	Office of Public Instruction
<i>Meeting Minutes Recorded by: Samantha Cooley, SITSD</i>	

Meeting Guests	
Name	Agency/Affiliation
John Burrell	DOJ-MATIC
Rebecca Cooper	FWP
Wendy Friedrich	DHS
Bill Genzoli	Xerox
Dale Gow	LEG
Kevin Kauska	MDT
Larry Krause	DOC
Suzi Kruger	DOR
Mazanec, Mike	OCHE
Meagher, Terry	DOC
Norman, Curt	OPI
Rivera, Sean	SITSD
Temple, Dawn	FWP
Temple, Dustin	FWP
Wetzel, Lance	MDT

# Montana Information Security Advisory Council

## Meeting Minutes July 15, 2015

Real-time Communication	
Name	Agency
Rick Bush	TRS
Chelini, Dan	DEQ
Dolan, Andrew	MS-ISAC
Edelman, Adam	MSU Security Officer
Jason Emery	Missoula County
Sky Foster	AG
Hammer, Evan	MSL
Michael Jares	DEQ
Arlitsch Kenning	MSU Library
Kim Moog	DLI
Angie Riley	MPERA
Joshua Rutledge	Montana School for the Deaf
Jacklynn Thiel	DPHHS
Lisa Vasa	SITSD-ESP
James Zito	SITSD-ISB

### I. Call to Order, Overview of ISAC and Introductions

Lynne Pizzini, Deputy CIO and CISO for SITSD welcomed the group. Meeting information and handouts provided are available [online](#) on the SITSD website. Today is a planning meeting. The primary purpose is to review the Operating Rules and Goals and Objectives.

### II. Operating Procedures

The Operating Procedures for this council were derived from other boards and councils within SITSD and modified to fit the needs and objectives of MT-ISAC. Please provide comments, suggestions or concerns while reviewing the documents today.

**★ See attachment 1: MT-ISAC Operating Rules and Goals and Objectives Review Table for all changes made to the MT-ISAC Operating Rules and MT-ISAC Goals and Objectives made during this meeting.**

**Overview: no comments provided**

#### **Responsibilities**

This section was developed from the Executive Order signed by Governor Bullock.

*Inquiry, Kreh Germaine:*

“‘Provide technical and managerial assistance’ what is that intended to describe?”

*Response, Lynne Pizzini:*

# Montana Information Security Advisory Council

---

## Meeting Minutes July 15, 2015

“The intention from the ITMC task force is that teams will be formulated through ISAC to assist state agencies in implementing security requirements and controls”

**Action:** Sherri Davidoff suggested ISAC will be referred to as “MT-ISAC” to avoid confusion, with “ISAC” being a commonly used acronym in the IT industry.

*Inquiry, Joe Chapman:*

“What is intended by ‘communications procedure’?”

*Response, Lynne Pizzini:*

“The intention of that bullet point was to establish a procedure for sharing information, at the request of the ITMC Task Force. One of the work groups from MT-ISAC will be tasked with developing and presenting a process from which information will be shared for this group. The objective is to share information in a uniform manner.”

*Inquiry, Joe Chapman:*

“What is the intent behind ‘conducting internal evaluations’?”

*Response, Bryan Costigan*

“Audits will not be a part of this process. Major Quinn’s area and the National Guard have evaluation teams that can conduct these evaluations for us. We are taking that option into consideration.”

### **Membership and Participation**

#### ***Nondisclosure Agreements (NDA)***

Due to the sensitive nature of the material being discussed in these meetings, all member’s and trusted delegate’s will be asked to sign non-disclosure agreements in the instance there are closed door sessions.

**Action:** Joe Frohlich will send a draft NDA to the group for review.

### **Voting**

*Inquiry, Joe Chapman:*

“Given this group is ‘advisory’ in nature and we vote, what happens after we vote? Is Ron delegated with authority to approve what we vote on or does it go to the Governor’s Office? On tactical issues we have to be agile in order to get things done.”

*Response, Ron Baldwin:*

“Like other advisory councils, the decisions we make here and consensus of the group carry weight. This weight increases the speed in which legislation, bills and policy we are involved with get enacted. Governor Bullock will be paying close attention to what is discussed and decided by this council, taking the recommendations of this group seriously.”

# Montana Information Security Advisory Council

---

## Meeting Minutes July 15, 2015

### Council and Member Participation

This council does allow members to select a designee. NDA's signed by members and delegates are permanent agreements. Designee's should be trusted individuals that play a significant role under council members.

**Action:** Provide designee information to Joe Frohlich as soon as possible.

Bryan Costigan commented that Montana is an open state as far as records and meetings. It is very important to keep that in mind in everything we do, leaning towards open discussions as much as possible.

### Security Rep. Participation

No comments/questions

### SITSD Participation

No comments/questions

### Communications

*Inquiry, Kreh Germaine:*

"We are an advisory council to the Governor, our vote is a consensus, is ITB taking our consensus, the State CIO or a combination of the two?"

*Response, Ron Baldwin:*

"All of the above. This council will discuss and vote on things of influence. The ITB will want to know what this council is discussing and advising, Lynne Pizzini will be providing that information to the ITB. One possibility is the things that are voted on by this council will be taken by an authoritative party. The Governor is the highest authoritative party we are working for here. We are all working for the citizens of Montana. We are here because we all very much care about security. The credibility of this group stands for itself and will be heard wherever it goes."

### Meetings and Meeting Times

This council is scheduled on the third Wednesday of every month, however, we are open to rescheduling. Sherri Davidoff commented that an 8:30 am meeting will make it difficult for people traveling across the State to get here. Rescheduling to an afternoon meeting will make it easier for those traveling. Rep. McCarthy agreed afternoon would be a better meeting time for the group.

**Action:** reschedule the meeting for 1:00 pm the third Wednesday of each month.

# Montana Information Security Advisory Council

---

## Meeting Minutes July 15, 2015

### **Staffing**

This section provides information on staff that will be provided from SITSD to help with administrative duties for the meeting. Maura Fleetwood and Samantha Cooley will fill these roles.

### **Effective**

The documents and information discussed at today's meeting will be voted on at the August meeting. All of the changes discussed today will be updated and reviewed in August.

**Action:** send additional changes to Lynne Pizzini or Joe Frohlich.

### **III. Goals and Objectives**

Lynne Pizzini provided the history of where the MT-ISAC Goals and Objectives came from. At the end of March, the National Governor's Association asked each Governor to put together a cybersecurity team to attend the National Governors Association Cybersecurity Summit. Ron Baldwin, Lynne Pizzini, Bryan Costigan, General Fox, and Butch Huseby were selected by Governor Bullock to represent Montana. At the conference they were asked to put together information about cybersecurity for our state and present a plan to the Governor on the following, three major areas of cybersecurity:

1. Governance
2. Posture
3. Response

The Governor agreed to the ideas presented in their plan, which are reflected in the Goals and Objectives document under review today. In addition, recommendations from the Cybersecurity Task Force and the Enterprise Risk Assessment were incorporated in the Goals and Objectives.

### **Goals/Mission**

*Inquiry, Kreh Germaine:*

“What is going to be our definition of ‘Montana Information Systems’? Is it just State government systems or does it expand out? Do we have a responsibility to the private sector on security?”

*Response, Lynne Pizzini:*

“The goal is to ensure the security of all information systems. Our primary focus is on state government systems with the intent of expanding in the future. We do not have a responsibility to the private sector as an advisory group. Our role will be to provide resources with information and training. We will not be putting mandates on private sector security systems.”

# Montana Information Security Advisory Council

---

## Meeting Minutes July 15, 2015

Homeland Security is testing private sector information systems and making recommendations to improve the security posture for those systems.

Erika Billiet commented that local governments will be using the policies developed in this group, she will distribute them to her contacts.

The term “cybersecurity” was removed from the language within the documents because it’s not just information systems, it is the physical aspect as well.

Kreh Germaine commented we are an advisory council to the Governor, if we are going to do our job well we have to keep in mind the mission and business of the government in the State of Montana. MT-ISAC’s mission should reflect that we want to ensure the business of the State is being done in a secure way.

### **Goals**

No Comment

### **Objectives**

### **Governance**

Adrian Irish commented the transition through the bullets starts to get off topic from governance there are some items that may be better categorized as “Posture”.

Major Quinn suggested that aside from “Governance, Posture and Response” there should be a fourth key concept that takes into consideration the needs of MUS, other agencies, local businesses and primarily, ties all this information together.

Joe Chapman inquired where “risk” is included and expressed the importance of balancing security with operations and cost. Lynne Pizzini suggested risk be added to “Posture”.

*Inquiry, Joe Chapman:*

“What is the intent behind ‘develop standard accountability processes for the department heads to ensure cybersecurity’?”

*Response, Bryan Costigan, Lynne Pizzini:*

“That bullet item was recommended by the group that attended the Cybersecurity Summit. We are developing processes to make it easier for department heads to be accountable for the portion of the law that says they are responsible for the security of their data. The intent of the bullet point is to stress the importance of the issue. An MT-ISAC subgroup will work address this issue further.”

# Montana Information Security Advisory Council

---

## Meeting Minutes July 15, 2015

### Posture

Kreh Germaine suggested removing items that refer to “implementing” programs given the role of this group is advisory. We want to be involved in developing a framework and advising, any role on implementing belongs elsewhere.

The group discussed the campaign to deliver the message of cybersecurity in the State. Bryan Costigan commented that a public relations campaign is important enough to have its own bullet. Currently, Lynne Pizzini shares awareness information with people outside of state government on a regular basis. The bullet point will be updated to reflect support and participation in statewide information security groups and leveraging of existing communication channels.

*Inquiry, Margaret Kauska:*

“Where does SANS fit in with ‘security training’?”

*Response, Joe Frohlich:*

“We are working on developing technical and managerial training for all agencies at least once a month at various locations across the state. SANS training is training for individuals and will continue.”

Sherri Davidoff commented she would like to see us develop our own training programs that are relevant to our specific needs and quit sending the money out of state.

*Inquiry, Adrian Irish:*

“Please elaborate on ‘the dashboard’.”

*Response, Lynne Pizzini*

“The state of Washington has a cybersecurity dashboard they provide to their Governor. We are developing one similar to that. Currently, we provide a monthly incident report, however, we want to expand by implementing the dashboard and executing best practices.”

**Action:** send any further comments on “Posture” to Joe Frohlich.

### Response

Sherri Davidoff suggested adding information on best practices for cybersecurity insurance and expressed the importance thereof. There has been a great deal of inquiry within the private sector on cybersecurity insurance and whether or not it is worth the cost. Ron Baldwin agreed cybersecurity insurance should be included. Ron was asked to speak at NASCIO on that topic. He suggested this council could produce an FAQ document and/or white paper on cybersecurity insurance. Stuart Fuller and Lynne Pizzini will help with this.

# Montana Information Security Advisory Council

---

## Meeting Minutes July 15, 2015

We are going to incorporate these suggestions and send the updated Operating Rules and Goals and Objectives prior to the next meeting.

### IV. Enterprise Security Policies, Joe Frohlich

Today the Enterprise Security Program (ESP) is submitting to the MT-ISAC five new Enterprise Security Policies based off of the NIST (National Institute of Standards and Technology) framework. The policies will be available online at the [ISAC website](#).

In February, 2013, President Obama issued an Executive Order “Improving Critical Infrastructure Cybersecurity” calling for risk-based cybersecurity framework and the implementation of best practices to manage cybersecurity risks. From this order, NIST provided a voluntary framework. NASCIO and the National Governor’s Association have been urging states to adopt the NIST Cybersecurity Framework since its release in 2014.

Montana is adopting the NIST cybersecurity framework. There are three main components:

1. Implementation Tiers
  - a. Organizations maturity level on risk management
2. Framework Core
  - a. Set of cybersecurity activities, outcomes and references (based on existing best practices)
  - b. Enterprise Security Policies are based on Framework Core
3. Framework Profile
  - a. Where we are today, roadmap for tomorrow (snapshot in any given category)

NIST Framework Core 5 main functions:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

Each function has a unique identifier and the categories are associated with each function. The description for each function is also describing each policy.

**Identify:** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Categories within this function include: Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategies.

# Montana Information Security Advisory Council

---

## Meeting Minutes July 15, 2015

**Protect:** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. Function supports the ability to limit or contain the impact of a potential cybersecurity event. Categories within this function include: Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology.

**Detect:** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. Function enables timely discovery of cybersecurity events. Categories within this function include: Anomalies and Events, Security Continuous Monitoring and Detection Process.

**Respond:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. Categories within this function include: Response Planning, Communications, Analysis, Mitigation and Improvements.

**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 major cybersecurity event. Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Categories within this function include: Recovery Planning, Improvements and Communications.

The framework is setup beginning with function, moving to category, then to subcategory and finally, to informational references. The 5 Core Functions tie to Montana's Baseline Security Controls. The identifier "PS" is for "Personnel Security" and the identifier "PM" is for "Program Management". There are 18 families within NIST 800-53 R4.

As you are reading through the policies, know that they reflect directly back to the Cybersecurity Core Functions.

*Inquiry, Stuart Fuller:*

"Last time we revised security policies there was a gap, how are we going to reduce this gap in case of an audit?"

*Response, Lynne Pizzini:*

"These five policies are from Montana's baseline security controls we adopted a couple of years ago. We are moving them into five policies that address the new cybersecurity framework and bring us into alignment with that. These will also be available for agencies to use internally as templates. All of the old policies are incorporated into the baseline security controls and we will be coming back to this group to ensure there are no gaps. There will be a document that shows where each of the old policies go into the baseline."

The proposed policies affect anything under the Montana Information Act, which are most state agencies. Some of the federal requirements ask that individual agencies have their own policies even though there are enterprise policies in place. We want to ensure agencies have the capability of being in compliance with requirements.

# Montana Information Security Advisory Council

---

## Meeting Minutes July 15, 2015

*Inquiry, Dan Chelini:*

“Do these policies affect everyone using SummitNet?”

*Response, Ron Baldwin:*

“Yes and municipalities and everyone connected to them.”

We are harmonizing with national standards and national initiatives and pulling them in to Montana. These will be foundational to how we consider security in this group from a policy perspective.

### **How do agencies adopt the Five Core Security Policies?**

The enterprise policies form the foundations of all policies, agencies can adopt policies that are more restrictive, but not something that is less restrictive unless an exception request is obtained through the DOA.

**Action:** review “[5 Core Security Policies](#)” for discussion prior to the next MT-ISAC Meeting.

### **V. Overview of Montana Analysis and Technical Information Center, Bryan Costigan**

There are two DOJ reps, Bryan Costigan, representing the enforcement side and John Burrell, the analyst assigned to cybersecurity threats affecting Montana. MATIC is the State Fusion Center, there are 17 around the nation. The primary purpose of the Fusion Center is to provide information on threats to critical infrastructure. Cybersecurity threats are growing in Montana. We provide information to people that can act on that information. MATIC shares information in every direction, top to bottom and side to side.

In the MATIC test environment we share information with DOJ, Department of Criminal Investigation, DOC, Helena Police Department and the Department of Homeland Security. MATIC wants information from MT-ISAC to share and prevent threats from taking place. MATIC will play a major role in developing MT-ISAC protocols for sharing information.

In the business we are in, the faster we get information, the faster we can address it, protect the State and prevent threats from reoccurring. Cost analysis shows the quicker information is shared, the less costly it is in the end.

MATIC receives information from other Fusion Centers and from the Federal Government. They will be sharing information with the DOA, local law enforcement and local agencies. Events in Montana are reported to MATIC, who then reports to Homeland Security.

Please share any cyber incidents with MATIC including:

- SPAM
- Phishing attempts
- Breaches

# Montana Information Security Advisory Council

---

## Meeting Minutes July 15, 2015

- Nefarious IP addresses

### **MATIC Contact Information:**

☎ 406-444-1330

✉ [dojintel@mt.gov](mailto:dojintel@mt.gov)

*Inquiry, Sherri Davidoff:*

“Can information security professionals in the private sector get the information being shared?”

*Response, Brian Costigan, Lynne Pizzini:*

“A couple years ago we started down this road, but it never took off. We are going to figure out how to best share information with the private sector. We have relationships with the power companies etc.”

“Part of the communication process can develop a communication mechanism to share information like that.”

The MT-ISAC Communications Subgroup will be very important. We can standup that group next month. We are not looking to reinvent the wheel but looking to things we do well amongst us and bringing it here to share. MATIC will be very helpful for setting the stage and the foundation for the communications process.

### **VI. Open Forum**

Ron spoke with the Governor’s Office yesterday, they are in the process of reviewing the MT-ISAC materials submitted and we expect to hear back from them soon.

### **Future Agenda Items:**

- ▲ Vote on the Operating Rules and Goals and Objectives,
- ▲ Formulate Subgroups
- ▲ Discuss the “5 Core Security Policies”.

**Action:** submit agenda items or subgroup ideas to Joe Frohlich or Lynne Pizzini.

### **Announcements:**

- ▲ If you would like to be on the mailing list to receive information on MT-ISAC, send Joe Frohlich an email request.
- ▲ The upcoming Cybersecurity Conference is on November, 18 at Fort Harrison.

# Montana Information Security Advisory Council

---

## Meeting Minutes July 15, 2015

▲Tech Junction is tomorrow in Bozeman with a focus on cybersecurity. Lynne Pizzini is the afternoon keynote speaker.

VII. **Public Comment: none**

VIII. **Adjourn: 10:49 am**

### Next Meeting Information:

**Date:** August 19, 2015

**Time:** 1:00 p.m.

**Location:** Montana State Capitol, room 152

### IX. **Summary of Action Items**

**Action:** ISAC will be referred to as “MT-ISAC” to avoid confusion, with “ISAC” being a commonly used acronym in the IT industry.

**Action:** Joe Frohlich will send a draft NDA to the council for review.

**Action:** Provide designee information to Joe Frohlich as soon as possible.

**Action:** reschedule the meeting for 1:00 pm the third Wednesday of each month.

**Action:** send additional changes/comments on Operating Rules and Goals and Objectives to Lynne Pizzini or Joe Frohlich.

**Action:** review “[5 Core Security Policies](#)” for discussion prior to the next MT-ISAC Meeting.

**Action:** submit agenda items or subgroup ideas to Lynne Pizzini or Joe Frohlich.

### X. **Attachments**

***Attachment 1: MT-ISAC Operating Rules and Goals and Objectives Review-Table of Changes***

***Attachment 2: ISAC Operating Rules***

***Attachment 3: ISAC Goals and Objectives***

***Meeting Minutes Draft Submitted by: Samantha Cooley  
July 23, 2015***

# Montana Information Security Advisory Council

## Operating Procedures and Goals and Objectives Review July 15, 2015

Document Title	Section of Document	Original Statement	Updated Statement and Justification (as needed)	Proposed by:
Name of Council		“ISAC”	“MT-ISAC” to eliminate any confusion given “ISAC” is a commonly used acronym in the IT industry	Sherri Davidoff
Operating Procedures	Responsibilities of the Council	“Develop an interagency security strategy with initiatives, priorities, policies, standards, and roles and responsibilities to enhance the State information security posture;”	Include the terminology “goals and objectives”	Joe Chapman
Operating Procedures	Responsibilities of the Council	“provide technical and managerial assistance relating to information technology security”	“Coordinate” rather than “provide”	Kreh Germaine
Operating Procedures	Responsibilities of the Council	“Establishing a communications procedure for receiving input from and sharing information with the public and the various agencies”	“Establish a communications process for sharing information with the public and the various agencies”	Joe Chapman
Operating Procedures	Responsibilities of the Council	“Conduct internal evaluations of the statewide security program”	“Recommend, oversee and review evaluations of the statewide security program”	Joe Chapman Bryan Costigan

## Montana Information Security Advisory Council

### Operating Procedures and Goals and Objectives Review July 15, 2015

Document Title	Section of Document	Original Statement	Updated Statement and Justification (as needed)	Proposed by:
Operating Procedures	Membership and Participation (Non-Disclosure Agreement)	“Each council member will have to sign a confidentiality agreement to encourage open discussion in an event of a closed door meeting.”	Council agreed to sign a NDA. The group agreed that the NDA must be signed by trusted delegates as well. This will be a permanent NDA as long as the council member/delegate is serving.	Lynne Pizzini/ Ron Baldwin
Operating Procedures	Meetings	“The council regular meetings are held on the third Wednesday of every month from 8:30 am until approximately 10:30 am.”	“The council regular meetings are held on the third Wednesday of every month from 1:00 pm until approximately 3:00 pm.”	Rep. McCarthy Sherri Davidoff, Adrian Irish
Operating Procedures	Effective	“These procedures will become effective upon approval at the July 2015 meeting.”	“These procedures will become effective upon approval at the August 2015 meeting.”	Joe Frohlich
Goals & Objectives 2015 Biennium	Mission	“.....as well as incorporate security into Montana’s information systems to ensure resilience.”	“.....as well as incorporate security into Montana’s information systems to ensure resilience to facilitate business in government operations.”	Kreh Germaine, Joe Chapman
Goals & Objectives 2015 Biennium	Goals/Governance		Include the definition of the security triad which is confidentiality, integrity and availability.	Adrian Irish

## Montana Information Security Advisory Council

### Operating Procedures and Goals and Objectives Review July 15, 2015

Document Title	Section of Document	Original Statement	Updated Statement and Justification (as needed)	Proposed by:
Goals & Objectives 2015 Biennium	Goals/Governance	“Advance Montana’s overall security <b>Governance</b> by adopting a framework of standards and processes.”	“Advance Montana’s overall security <b>Governance</b> by adopting frameworks of standards and processes.”	Sherri Davidoff
Goals & Objectives 2015 Biennium	Objectives/Governance	<p>“Understand the value of the University System’s security needs”</p> <p>“Understand the value of the Local Government security needs”</p> <p>“Understand the value of the Montana Local Business security needs”</p>	<p>“Recognize the University Systems security needs”</p> <p>“Recognize the Local Government security needs”</p> <p>“Recognize Montana Local Business security needs”</p>	Ron Baldwin Joe Chapman
Goals & Objectives 2015 Biennium	Objectives/Governance	“Formalize information sharing protocol and document standing information needs between HAS, DOA/SITSD/CISO, and DOJ/DIC/MATIC.”	“Formalize information sharing protocol and document standing information needs.”	John Daugherty
Goals & Objectives 2015 Biennium	Add a new key concept		Add a fourth key concept, such as “coordination” or “facilitation” that falls out separately from the Governance piece.	Major Quinn

## Montana Information Security Advisory Council

### Operating Procedures and Goals and Objectives Review July 15, 2015

Document Title	Section of Document	Original Statement	Updated Statement and Justification (as needed)	Proposed by:
Goals & Objectives 2015 Biennium	Objectives/Governance	<i>*add a new bullet point</i>	“Consider the needs of public information, access to public information, and the continuity of doing business in the State of Montana when making recommendations relative to security”	Ron Baldwin
Goals & Objectives 2015 Biennium	Objectives/Governance	“Develop standard accountability processes for department heads to ensure cybersecurity.”	“Develop standard accountability processes for department heads to ensure information security.”  This was put in to stress the importance of dept. heads being accountable for their agencies information security.	Joe Chapman
Goals & Objectives 2015 Biennium	*Add appendices		Add NIST glossary of terms and definitions to the end of the document. This will include definitions of cybersecurity and information security.	Bryan Costigan
Goals & Objectives 2015 Biennium	Entire document	“cybersecurity” throughout the document	Change to “information security” throughout the document	Lynne Pizzini

## Montana Information Security Advisory Council

### Operating Procedures and Goals and Objectives Review July 15, 2015

Document Title	Section of Document	Original Statement	Updated Statement and Justification (as needed)	Proposed by:
Goals & Objectives 2015 Biennium	Objectives/Governance	“Implement an Enterprise Security Program in conjunction with the ISAC to ensure effective implementation of cybersecurity in all agencies of state government”	Change wording to reflect the advisory role of the ISAC , replace “implement”.	Kreh Germaine
Goals & Objectives 2015 Biennium	Objectives/Governance	“Establish through Executive Order an Information Security Advisory Council (ISAC) that includes state, local, National Guard, and private sector representation.”	Remove from document.	John Daugherty
Goals & Objectives 2015 Biennium	Objectives/Posture	<i>*add a new bullet point</i>	“Identify key players within industry sectors and provide a forum for developing guidance and communicating with industry sectors.”	Sherri Davidoff
Goals & Objectives 2015 Biennium	Objectives/Posture		Add information about “risk”	Joe Chapman
Goals & Objectives 2015 Biennium	Objectives/Posture	“Support a statewide cybersecurity training program to serve technical and managerial needs”	“Support a statewide information security training and awareness program to serve technical and managerial needs”	Lynne Pizzini
Goals &	Objectives/Posture	<i>*add a new bullet point</i>		Sherri Davidoff

## Montana Information Security Advisory Council

### Operating Procedures and Goals and Objectives Review July 15, 2015

Document Title	Section of Document	Original Statement	Updated Statement and Justification (as needed)	Proposed by:
Objectives 2015 Biennium			“Support and participate in statewide information security groups and help to facilitate and leverage the existing communications channels we have.”	
Goals & Objectives 2015 Biennium	Objectives/Posture	“Support a statewide cybersecurity training program to serve technical and managerial needs”	“Support a statewide cybersecurity training program to serve technical and managerial needs and SANS program for individuals”	Margaret Kauska
Goals & Objectives 2015 Biennium	Objectives/Posture	“Establish a communications procedure...”	“Establish a communications process...”	Bryan Costigan
Goals & Objectives 2015 Biennium	Objectives/Posture	“Develop and implement a State Risk Management Services Program.”	“Develop and implement a State Risk Management Services Program and share risk management guidance and recommendations with Local Government and the private sector.”	Erika Billiet
Goals & Objectives 2015 Biennium	Objectives/Posture	Explore training of DOA/DOJ/National Guard staff to defend against cybersecurity attacks through the use of State of Washington National Guard cyber unit.	“Explore training of DOA/DOJ/National Guard staff to defend against cybersecurity attacks through the use of best practices within the State of Washington National Guard cyber unit.”	Joe Chapman

## Montana Information Security Advisory Council

### Operating Procedures and Goals and Objectives Review July 15, 2015

Document Title	Section of Document	Original Statement	Updated Statement and Justification (as needed)	Proposed by:
Goals & Objectives 2015 Biennium	Objectives/Response	<i>*add a new bullet point</i>	Add information on best practices for cybersecurity insurance, recommendations, options, awareness, coverage, cost, etc.	Sherri Davidoff
Goals & Objectives 2015 Biennium	Objectives/Response	“Recommend resources (funding, people, etc.) and possible methods to obtain cybersecurity teams, in order to enhance the State information security posture.”	This element is overarching throughout all parts of the program, move it to “Objectives/Governance” section or into the fourth key concept previously suggested.	Joe Chapman
<i>Document review changes recorded by: Samantha Cooley July 15, 2015</i>				

# 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.