

# Montana Information Security Advisory Council

## Meeting Minutes August 19, 2015

Attendees	
<i>Meeting Chairperson: Ron Baldwin</i>	
<b>Name</b>	<b>Affiliation</b>
Erika Billiet	Department of Revenue
Joe Chapman	Department of Justice
Bryan Costigan	MATIC/Department of Justice
John Daugherty	Department of Corrections
☞ Sherri Davidoff	LMG Security
Kreh Germaine	Department of Natural Resources and Conservation
Manuel Soto	Office of Public Instruction
Margaret Kauska	Department of Revenue
Lynne Pizzini	State Chief Information Security Officer
<i>Minutes recorded by: Samantha Cooley</i>	

### Meeting Guests

Rebecca Cooper, FWP; John Burrell, MATIC-DOJ; Eric Durkin, Northrup Grumman; Tiffany Ferguson, Northrup Grumman; Tom Maderville, DOR; Lance Wetzell, MDT; Chris Silvonen, DPHHS; Edward Sivils, SITSD; Mark Van Alstyne, SOS; Mike Bousliman, MDT; Aubrey Curtis, LAD; Dale Gow, LEG; Christi Mock, DPHHS; Wendy Friedrich, DPHHS; Joe Frohlich, SITSD

### ☞ Real-time Communication

Larry Krause, DOC; Dan Chelini, DEQ; Brad Flath, SOS; Judy Kelly, DLI; Cyndie Lockett, LEG; Angie Riley, MPERA; Jerry Marks, SITSD

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

Ron Baldwin welcomed everyone to the first official meeting. The council members were approved by the Governor, this council was formed by Executive Order. Governor Bullock will be in attendance at the September meeting to say a few words.

### II. Operating Procedures

The operating procedures were updated with all of the changes suggested during the last meeting. Ron asked the group for feedback on additional changes. Kreh Germaine commented that there are still some references to “cybersecurity”, these should be changed to “information security”.

# Montana Information Security Advisory Council

---

## Meeting Minutes August 19, 2015

**Motion:** The motion to approve the Operating Procedures, amended, was made. Bryan Costigan approved the motion, with John Dougherty seconding the motion. The group was in favor, the motion carries.

### Non-Disclosure Agreement

**Motion:** The MT-ISAC Non-Disclosure Agreement was approved.

### III. Goals & Objectives

The updated Goals and Objectives were reviewed. Joe Chapman recommended a work group be formed to make additional updates.

#### Goals and Objectives Work Group Proposal (Joe Chapman):

- Solidify the Goals and Objectives
- Reconsider adding “Situational Awareness”
- Further clarify and define
- Consolidate and reduce the number of objectives
- Create better flow within the document
- Address language that conflicts with the advisory role of MT-ISAC

#### Additional Considerations (group comments):

- “Situational Awareness” is part of several areas, this was recommended to be included during the last meeting and is considered overarching.
- The Goals and Objectives originated from the Governor’s recommendations.
- MT-ISAC needs to be expeditious in setting Goals and Objectives.

#### Options:

1. Accept the Goals and Objectives today as-is and then come back and refine them in a few months.
2. Approve the goals today and let the Work Group update the objectives.
3. Go back to the drawing board as a council in a working session
4. Formulate a Work Group to revisit the Goals and Objectives and complete the revisions within the next three weeks, to be presented to the council at the September MT-ISAC Meeting.

**Motion:** Ron Baldwin called for a motion. Joe Chapman proposed option four, to formulate a Work Group to complete the task within the next three weeks. Bryan Costigan seconded the motion and the group was in favor, he motion carries.

# Montana Information Security Advisory Council

---

## Meeting Minutes August 19, 2015

**Action:** The Work Group will meet within the next three weeks to have the Goals and Objectives ready to present at the September MT-ISAC Meeting. The group members are: Joe Chapman, Kreh Germaine, Adrian Irish, Margaret Kauska and Joe Frohlich.

### IV. Enterprise Security Policies

Currently, there is a security policy in place containing around 200 NIST controls. Joe Frohlich is working on combining 29 security policies into the overarching NIST controls and the five Enterprise Security Policies. The five new, consolidated policies are “Identify”, “Detect”, “Protect”, “Respond” and “Recover”.

*Inquiry, Bryan Costigan:*

“Are these replacing the current policies or combining them?”

*Response, Joe Frohlich:*

“This is a combination of everything. The goal is to move from 29 policies to six. They tie to NIST 800-53, which the state already adopted, several years ago.”

*Inquiry, Bryan Costigan:*

“As these come in, do they push the old ones out?”

*Response, Joe Frohlich and Lynne Pizzini:*

“Once the updated baseline has been approved, the 28 policies will be removed.”

–Joe Frohlich

“The five policies being proposed are being recommended to follow the new cybersecurity framework recommended by NIST. They are being used by agencies as templates that require federal mandates. They are pulled from common controls for agency use. These are new, consolidated, policies, however, there is no new information within them. They are simply in a more consolidated, easy to use, format.”

- Lynne Pizzini

*Inquiry, Kreh Germaine:*

“I remember there was a discussion about a Data Classification Policy, is that wrapped in here?”

*Response, Joe Frohlich:*

“No, that is not a security policy, it is, however, referenced in the Baseline Controls. It is an enterprise policy that is being proposed from the CIO’s office, recommending that agencies classify their data. It has security implications. That is why it is being reviewed by ITMC, not this group.”

# Montana Information Security Advisory Council

---

## Meeting Minutes August 19, 2015

Ron Baldwin commented this is a good move for the State. A few years ago the State approved the NIST Framework, those 29 policies are now being merged into six. The objective is to be clear, concise, consolidated and effective. These six policies represent the Cybersecurity Framework. The controls within them refer back to the previous policies. This will be useful in dealing with the federal government.

Joe Frohlich presented an overview of the Baseline Security Control's. The document ties 800-53 Rev.4 to each policy, going from policy, to function, to category and finally, subcategory.

*Inquiry, Joe Chapman:*

“There is a lot of work being proposed here. Do you want comments/feedback on this? How are we going to roll all of these out and enforce them?”

*Response, Joe Frohlich and Lynne Pizzini:*

“These policies are all within the Common Baseline Controls already, in appendix A, that has been in place for several years. This is simply another way to look at the Common Controls, 800-53. This is a nice way to spell out what is required. The Baseline Controls are more prescriptive for the agencies, these five policies are meant to be templates for agencies. They are mirrors to one another.”

–Joe Frohlich

“Everything in these policies is already in the Enterprise Security Policy. To answer how these are going to be implemented: that is why this group was formed, to begin implementing the policies statewide.

-Lynne Pizzini

*Inquiry, Bryan Costigan:*

“Should all of work relate back to these Five Policies and NIST?”

*Response, Lynne Pizzini:*

“Yes, if you look at the objectives they do relate back. We can relate each one back to one of the five policies.”

Today was a review and discussion of the five policies, if need be, the committee can vote on them in September. If there is no objection, we can vote on them today.

*Inquiry, Kreh Germaine:*

“I understand where Joe's concerns are coming from. One of my concerns is how are we to obtain the resources to fulfill these requirements? How do we know we

# Montana Information Security Advisory Council

---

## Meeting Minutes August 19, 2015

are in 100% compliance? How do we adopt something like this without overwhelming the agency?"

*Response, Lynne Pizzini and Joe Frohlich:*

"One of the recommendations from the Task Force was to create teams to assist with implementing the controls. We need to make sure we are giving the agencies the tools to do that."

-Lynne Pizzini

"The Framework, the Baseline, the 800-53, they are *goals*. This is the framework we want to achieve, we have had them in place for years now. They are goals and objectives we wish to reach, this is a long-term goal. We should make notes of where agencies, the enterprise isn't in compliance with certain policies and then make a plan to get there. We are not close to these five, or the baseline, this is a roadmap for the future."

-Joe Frohlich

### Challenges/Concerns:

1. **Protecting Information:** Vulnerabilities will be identified, as we are trying to fix them through adaptation of this policy. We have tools in place, but no mechanism in place to identify when this information reaches a critical point, how do we protect it? What is the appropriate legal stance? There is concern that under the Sunshine Law, people could request this information from us and we would give them more than we should.  
-Bryan Costigan
2. **Audit/Impact on Insurance:** If we establish the requirements, knowing agencies cannot yet meet them, as they are long term goals, are we setting ourselves up for an audit? Will this cause an issue with our insurance if we set a standard we cannot meet? Changing the language to state "here are the requirements we are trying to obtain as a long term goal" may prevent issues from arising. -General Quinn
3. **Liability:** Has anyone on the DOA legal team reviewed these policies? Is this a good position for us to be in? -Kreh Germaine

### Solutions/Opportunities:

1. **Audit/Impact on Insurance:** DOR is governed by the IRS, they conduct an assessment every three years and this is what they *want* to see, they are looking for the NIST template. We have a draft policy, if we approve it, by no means are we saying we are going to implement it and have it done immediately. It is overwhelming, you have to break it down. What they are looking for is progress: action, milestones and realistic timelines. What the IRS and Feds are require of us is substantial. As long as we are making progress, we are headed in a good direction. This is a good place to start.

# Montana Information Security Advisory Council

---

## Meeting Minutes August 19, 2015

Resources are a huge issue, making strides towards this, one step at a time, is a good thing. – Margaret Kauska

I think that Stuart Fuller would echo this. Insurance companies ask whether or not a policy exists on how you protect data and systems, and if that policy is being followed. I can say our experience with the HHS incident proved that. A policy indicates a concerted effort to recognize something at a level that allows policy as a guideline. It is a very important thing, we hear this from the IRS, the Federal Government, the Publication 1075, HIPPA, FERPA, etc. Lynne is familiar with all of the Federal requirements, these are laws now, these are acts. The fines and implication of breaches are much greater, not having any policies in place is a major liability. –Ron Baldwin

2. **Policy Requirements and Risk Assessment:** Normally, when risk assessments are completed we utilize a policy to see where we are at in compliance with that policy. We used the Baseline Security Controls to conduct risk assessments. These five policies are already policies. We are not introducing anything new, they are already in the Baseline Security Controls. The Enterprise Risk Assessment recommended we update our policies to align them with the new NIST framework. This action fulfills that requirement.  
–Lynne Pizzini
3. **Liability:** It is much better to have policy than no policy at all, we need framework to achieve this. It is important for agencies to understand what all of this means. Agencies should be documenting on specific systems, their current status and identifying vulnerabilities and what risks there are. Overall goals need to be identified to protect these systems. It is up to the Security Officers and teams for the State to go through the systems and vulnerabilities, how to best protect and make sure these systems are covered.  
–Joe Frohlich

### **Outcome:**

Lynne and I were just chatting about this, one thing I want to point out, this relates to situational awareness, State policies... all policies, provide an awareness for the State on what we are supposed to do. We all have challenges with resources, people and funding. Policy provides structure. Kreh has a valid concern on liabilities, Erika has good suggestions, what I would like to suggest from this council, is that we undertake a legal review. The review will investigate the proposed policies considering the State's liability, State law and Federal law.

–Ron Baldwin

**Motion:** Establish a legal counsel to review the Enterprise Policies consisting of Mike Manion and the legal counsel from both DOR and DOJ. All were in favor. Motion passed.

**Action:** Move forward with legal opinion review and add this to the agenda for the next meeting.

# Montana Information Security Advisory Council

---

## Meeting Minutes August 19, 2015

### V. Baseline Security Controls, Joe Frohlich

Joe Frohlich presented an overview of the Baseline Security Control Appendices to the group. The table contains a control number to reference, control name, priority and control baseline.

To locate all of the policies within the new Baseline Security Controls, access these documents online at the [MT-ISAC website](#). This is a searchable document, intended for ease of use for incident response purposes.

**Action:** Joe Frohlich will send an email this week so everyone can review the Appendices and provide comments.

### VI. Formation of Suggested Workgroups, Ron Baldwin

The Goals and Objectives Work Group and the Legal Review Team will begin immediately.

1. Goals and Objectives: Joe Chapman (Chair), Kreh Germaine, Margaret Kauska, Adrian Irish, Joe Frohlich
2. Situational Awareness: Bryan Costigan (Chair), John Burrell, Sherri Davidoff, Lynne Pizzini, Dawn Temple, Kimberly McIntyre, Margaret Kauska, DOR Rep (unnamed), Military Affairs Rep (unnamed), Joe Frohlich
3. Public Safety: will discuss at the next meeting
4. Cyber Environment (Posture/Landscape): General Quinn, Sherri Davidoff, Joe Frohlich

All suggested Work Groups have been tabled until Goals and Objectives have been approved by the council. An exception has been made for the Situational Awareness Workgroup.

### VII. Current Threats, Sean Rivera

Sean presented an overview of current cybersecurity threats.

**Groups:**

Vikingdom  
Anonymous

**Trend in Attacks:**

Malvertising  
Android Certifi-gate  
Windows 2003 Server  
Out-of-Band Patch for IE

For more details on the information discussed about current threats, please contact Sean Rivera.

# Montana Information Security Advisory Council

---

## Meeting Minutes August 19, 2015

### VIII. Cybersecurity Month, Lisa Vasa

The theme for Cybersecurity Month this year will be “Stay Safe on the Information Highway”.

#### **SANS/ Cybersecurity Month Schedule:**

SANS Securing the Human Year End Reset: August 25-31

National Cyber Security Awareness Month: October 2015

Monthly Security Awareness Events: October 2015 – September 2016

SITSD is planning to roll out events in October. Events will include activities, giveaways and prizes for everyone. The goal is to have one event per month at different locations throughout the year to reach as many people as possible.

**Action:** Contact Lisa Vasa or Joe Frohlich if your agency is interested in hosting an event.

General Quinn offered the use of Fort Harrison as an event location.

*Inquiry, Bryan Costigan:*

“Is SITSD reaching out to the University System?”

*Response, Lisa Vasa:*

“At this point it’s been Helena locations only, we don’t have a large budget to travel. If there is a remote location, let us know, we will try to make it work.”

Adrian Irish was asked if they do anything similar to Cybersecurity Month for the University System. His response was that MSU has been doing a Security Conference, we thought we could hold an event. However, October can be a difficult month to secure speakers. They would like to do something given the student population is so vulnerable to Cybersecurity attacks.

Lisa Vasa commented SITSD wants to hold one event per month at different locations, we could do something for the University System another month, it doesn’t have to be October.

**Action:** Lisa Vasa will work with Adrian Irish to consider setting up an event for the Montana University System.

### IX. Open Forum

#### **National Guard Risk Assessment Teams, Major General Quinn**

General Quinn commented they are working on a policy that allows the National Guard Cyber Teams to work with private and public entities. It frees up the reins for the National Guard. General Quinn

# Montana Information Security Advisory Council

---

## Meeting Minutes August 19, 2015

will be traveling to Washington State. Washington has an aggressive National Guard Cyber Team Program that would be beneficial to learn more about. Sherri Davidoff commented this could be a great resource for the State.

**Action:** add Cybersecurity National Guard Teams to MT-ISAC Agenda for discussion after more work is done on this project.

### **Fort Harrison Cybersecurity Event, Erika Billiet**

The Fort Harrison Cybersecurity event date has changed to November 3, 2015. It will be held in the HHS auditorium. There are no definite details yet, there is a meeting next week to set the agenda, once that is done Lynne Pizzini will send out the information.

**Action:** Lynne Pizzini will send out Fort Harrison Cybersecurity event information.

Public Comment: none

### **X. Adjourn**

The meeting was adjourned at 3:05 pm.

#### **Next Meeting Information:**

**Date:** September 16, 2015

**Time:** 1:00 pm – 3:00 pm

**Location:** Capitol, room 152

### **XI. Summary of Action Items**

**Action:** The Work Group will meet within the next three weeks to have the Goals and Objectives ready to present at the September MT-ISAC Meeting. The group members are: Joe Chapman, Kreh Germaine, Adrian Irish, Margaret Kauska and Joe Frohlich.

**Action:** Move forward with legal opinion review and add this to the agenda for the next meeting.

**Action:** Contact Lisa Vasa or Joe Frohlich if your agency is interested in hosting an event.

**Action:** Lisa Vasa will work with Adrian Irish to (potentially) set up an event for the Montana University System.

*\*Summary of "Motions Passed" begins on page 10*

# Montana Information Security Advisory Council

---

## Meeting Minutes August 19, 2015

### XII. Summary of Motions Passed

**Motion:** The motion to approve the Operating Procedures, amended, was made. Bryan Costigan approved the motion, with John Dougherty seconding the motion. All were in favor, the motion carries.

**Motion:** The MT-ISAC Non-Disclosure Agreement was approved.

**Motion:** Ron Baldwin called for a motion. Joe Chapman proposed option four, the formulation of a Work Group to complete the task within the next three weeks. Bryan Costigan seconded the motion and the group was in favor and the motion carries.

**Motion:** Establish a legal counsel to review the Enterprise Policies consisting of Mike Manion and the legal counsel from both DOR and DOJ. All were in favor, the motion carries.

*Meeting Minutes Draft submitted by: Samantha Cooley  
September 1, 2015*