

Updated Recommendations to the Governor to Enhance the State of Montana's Cybersecurity Environment – 2017

In March, 2015, the National Governors Association held a Summit on State Cybersecurity where Montana representatives participated. From that summit, recommendations were made to Governor Bullock in May, 2015 which resulted in the creation of the Montana Information Security Advisory Council (MT-ISAC). MT-ISAC has diligently worked to enhance cybersecurity preparedness in Montana through updating policies, creation and implementation of best practices and other workgroup activities.

In March, 2017, the NGA held an additional summit on State Cybersecurity. The participating Montana representatives reviewed the recommendations from 2015 and have updated the status from the council work and are providing updated recommendations in this document.

ACCOMPLISHMENTS

Much work has been completed through the work of the MT--ISAC and the Enterprise Security Program that was developed by the State Information Technology Services Division. These are the highlights of the accomplishments:

- Establishment of the MT-ISAC through Executive Order that includes state, local, National Guard, legislative and private sector representation.
- Implementation of an Enterprise Security Program, through the use of the ISAC, for state government to ensure effective implementation of cybersecurity in all agencies of state government. The program is addressing gaps that focus on state resources.
- Updated state cybersecurity policies to align with the new Federal cybersecurity framework.
- Developed a cybersecurity situational awareness process for all users.
- Formalized an information sharing protocol and developed standing information needs between HSA, DOA/SITSD/CISO and DOJ/DCI/MATIC .
- Developed a standard accountability process for Department heads to ensure cybersecurity.
- Developed a Governor's cybersecurity dashboard.
- Have begun to assess security posture/readiness of each Department in State government. Developed an ongoing program to address cybersecurity risk.
- Explored training of DOA/DOJ/National Guard staff to defend against cyber-attacks through the use of the State of Washington National Guard cyber unit. Evaluated how we can apply this in Montana.
- Established communication with the private sector through current emergency communications contacts.

RECOMMENDATIONS

Continuing work in the critical area of cybersecurity is still a priority and has been identified to have three areas of focus. The following are recommendations in these areas from the 2015 meeting that are still outstanding, as well as some additional items that the participants would like to see addressed as a result of the recent meeting in March, 2017.

Governance

1. MT-ISAC needs to continue to address cybersecurity issues within state government. The council also needs to broaden its focus to assist with external related issues. In order to accomplish this recommendation, the make-up of the council should change with more members coming from the private sector and less from state government. This is a good opportunity to make this change as the membership renewal should be completed by July 1, 2017.
2. Understanding the value of the University System, we need to gain perspective of their cybersecurity preparedness and the threats that they face.
3. Update current state statutes, both administrative for state government needs and criminal, to address the present-day cyber security environment.
4. 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. Have one institution become a Center of Excellence for Cyber Education.
5. Complete a cost analysis for cybersecurity for the State of Montana. Include recommendations from other states and the Federal perspective on investment in cybersecurity.

Posture

1. Develop a process to deliver the message of cybersecurity in a positive and informational manner with an external focus that engages the listener to pay attention.
2. Continue to collaborate with private industry on understanding the cybersecurity posture of critical infrastructure.
3. Apply best practices identified in other states, including penetration testing, to the Montana unit of the National Guard. Have the National Guard perform penetration testing on state systems to identify risks.
4. Increase the education of Montana's law enforcement group regarding cybersecurity.
5. Invite private sector entities, including the utility companies, to participate in annual cyber table top exercise. Conduct a real time cyber exercise as soon as possible.

Response

1. Move forward with state preparedness and migrate toward evaluation of the role with private sector as time and resources allow.
2. Research and recommend criminal investigative response in coordination with HSA, DOA, DOJ, and FBI.
3. Explore additional resources in DOJ/DCI for Network Cyber Investigations.