

#	E, M, N	NIST	Priority	Current Objective	New Suggestion	G&O #	Notes
1	E	I	1	Governance - #2 bullet - Update State of Montana information security policies to align with the NIST Cybersecurity Framework.	Ensure State of Montana information security policies and documents align with the NIST Cybersecurity Framework.	1.1	
2	M	I	1	Governance - #3 bullet - Develop standard accountability processes for Department heads to ensure information security.	Develop and implement a statewide standardized assessment and measures for Departments and the State information security program.	1.2	From "accountability for dept. heads" under Governance
3	E	I	2	Posture - #10 Bullet - Conduct internal evaluations of the statewide information security program.	part of #2	1.2.1	
4	E	I	2	Response - #1 Bullet - Develop a Governor's information security dashboard	part of #2	1.2.2	
5	E	I	2	Response - #2 Bullet - Provide a yearly information security assessment to the Governor showing program successes and shortcomings with a plan to address shortcomings.	Provide a yearly State information security assessment to the Governor showing program successes and a plan to address shortcomings.	1.2.3	this should be tied to #2
6	M	I	1	Posture - #3 Bullet - Develop and implement a state Risk Management services program and share risk management guidance and recommendations with local governments and the private sector.	1.3. Implement a statewide standardized system risk management template (measures, authority to operate, etc) based on best practices	1.3	
7	E	I	3	Posture - #3 Bullet - Develop and implement a state Risk Management services program and share risk management guidance and recommendations with local governments and the private sector.	Share risk management guidance and recommendations with local governments and the private sector.	1.4	This is split out from Posture #3 Bullet
8	M	I	2	Response - #4 - Recommend new legislation or updates to existing laws such as reporting requirements to government and citizens as appropriate.	Recommend new legislation or update current statutes, administrative and criminal, to address the present-day information security environment.	1.5	modified a bit
9	E	I	3	Situational Awareness - #5 Bullet - Recognize the University System's security needs; Document the University System perspective of their information security preparedness and the threats that they face, help develop a strategy of best practices, and assist with how to best promote information security.	Recognize the University System's security needs;	Guiding Principle	
10	E	I	3	Situational Awareness - #6 Bullet - Recognize the Local Government security needs; Document the Local Government perspective of their information security preparedness and the threats that they face, help develop a strategy of best practices, and assist with how to best promote information security.	Recognize the Local Government security needs;	Guiding Principle	
11	E	I	3	Situational Awareness - #7 Bullet - Recognize the Montana Local Business security needs; Document the Local Business perspective of their information security preparedness and the threats that they face, help develop a strategy of best practices, and assist with how to best promote information security.	Recognize the Montana Local Business security needs.	Guiding Principle	
12	E	I	3	Situational Awareness - #8 Bullet - 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.		Guiding Principle	put into list of Guiding Principles
13	M	I	1	Governance - #1 Bullet?? Response #6?? Posture #4??	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.	1.6	combined with another Obj. How is this diff from "info sec teams" under Posture?
14	E	I	2	Situational Awareness - #11 Bullet - Identify key players within industry sectors and provide a forum for developing guidance and communicating with industry sectors.		1.9	
15	N	P	1	NEW	Identify location of sensitive data and methods to protect it.	2.11	
16	E	P	1	Posture - #7 Bullet- Develop strategy for better patch management	Develop and implement process for better patch management.	2.4	
17	E	P	1	Posture - #8 Bullet - Develop limited user rights strategy for state information systems.		2.5	

18	E	P	3	Posture - #9 Bullet - Identify legacy systems which exist on the State of Montana network and create a plan for securing or removing those systems.		2.6	
19	E	P	2	Situational Awareness - #9 Bullet - Encourage development of a trained and educated information security workforce in Montana through the University System with private sector input.		1.7	
20	E	P	3	Situational Awareness - #10 Bullet - Include an apprenticeship or internship program to develop hands-on information security skills.		1.8	Joe Frohlich Comment: Situational Awareness Bullet #9 and #10 are really tied together and could be combined somehow
21	N	P	1	NEW	Recommend software, hardware, services, processes, and resources to increase protection capabilities.	2.7	
22	M	P	1	NEW	Document standing threat/vulnerability needs/sources and determine fast, efficient, and secure sharing methods.	2.2.1	Situational Awareness Group
23	E	P	2	Posture - # 12 Bullet - Advise on security requirements in the specifications for solicitation of state contracts for procuring information technology resources.	Recommend security requirements for solicitation of and inclusion in state contracts involving information technology. (address breach language for contracts)	2.8	Added "breach" part
24	E	P	2	Response - #10 Bullet - Provide information on best practices for information security insurance, recommendations, options, awareness, coverage, cost, and other considerations.	Provide information on best practices for information security insurance , recommendations, (training) options, awareness, coverage, cost, and other considerations.	2.9	added "training"
25	N	P	1	NEW	Implement methods and/or tools to inventory authorized and unauthorized software .	2.10	from SANS top 20
26	N	P	1	NEW	Implement methods and/or tools to secure configurations on workstations and servers.	combined into 2.7	from SANS top 20
27	E	P	2	Response - #9 Bullet - Develop a plan to increase the education of Montana's law enforcement group regarding information security.		4.2.4	not sure what this means or why only them
28	M	P	1	Situational Awareness - Bullet #3 - Support a statewide information security training and awareness program to serve technical and managerial needs, as well as the needs of individuals.	Implement a comprehensive information security awareness and training program (users, IT staff, contractors, mtg)	2.1	
29	E	P	1	Situational Awareness - Bullet #13 - Explore training of DOA/DOJ/National Guard staff to defend against cyber-attacks through the use of best practices within the State of Washington National Guard cyber unit.		2.3.1	
30	E	P	1	Situational Awareness - Bullet #14 - Evaluate the State of Washington's best practices of the cyber unit of the National Guard and apply its practices in Montana where applicable.		2.3.2	combine with #29?
31	E	P	3	Response - #7 Bullet - Provide technical and managerial assistance relating to information security.		delete	who would do this and who would they do it for? Agencies?
32	E	P	2	Response - #3 Bullet - Foster better communication in information security between federal, state, local, and tribal governments.		2.2.2	
33	E	P	1	Situational Awareness - Bullet #12 - Collaborate with private industry to understand the information security posture of critical infrastructure.		1.10	
34	N	D	1	NEW	Recommend software, hardware, services, processes, resources, etc. to increase detection capabilities.	3.1	
35	N	R	1	NEW	4.1. Recommend software, hardware, services, processes, and resources to enhance agency and State incident response - tools, procedures, checklists, lessons learned, and guidelines	4.1	
36	E	R	1	Response - #8 Bullet - Improve the State of Montana's investigative expertise in the information security area.		4.2.1	
37	E	R	1	Situational Awareness - Bullet #15 - Explore additional resources in DOJ/DCI for Network Cyber Investigations.		4.2.2	same as #36?
38	E	R	2	Situational Awareness - Bullet #16 - Research and recommend criminal investigative response in coordination with HSA, DOA, DOJ, and FBI.		4.2.3	
39	E			Governance - Bullet #1 - 1. Develop an interagency information security strategy with initiatives, priorities, policies, standards, and roles and responsibilities to enhance the state information security posture.		This is the MISSION of the MT-ISAC	

40	E			Posture - Bullet #1 - Implement an Enterprise Security Program in conjunction with the MT-ISAC to advise on the effective implementation of information security in all agencies of state government.		this is incorporated in mission, goals and objectives	
41	E			Posture - Bullet #2 - Begin the enterprise program by addressing gaps focusing on state government and expanding to the private sector over time through the use of the MT-ISAC.		part Guiding Principle but part is not role of gov't	
42	E			Posture - Bullet #4 - Recommend resources (funding, people, etc.) and possible methods to obtain information security teams, in order to enhance the State information security posture.		1.6	
43	E			Posture - Bullet #5 - Formalize information sharing protocol and document standing information needs.		2.2.1	
44	E			Posture - Bullet #6 - Begin to assess security posture and readiness of each Department in state government.		1.2	
45	E			Posture - Bullet #11 - Recommend appropriate cost-effective safeguards to reduce, eliminate, or recover from identified threats to data.		2.5, 2.11, 5.1	
46	E			Response - Bullet 5 - Create recommendations to update current state statutes, both administrative statutes for state government needs and criminal statutes to address the present-day information security environment.		1.5	
47	E			Response - Bullet #6 - 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 MT-ISAC direction and industry best practices.		1.6	
48	E			Situational Awareness - Bullet #1 - Create a strategy to promote information security situational awareness for all users.		2.2.1	
49	E			Situational Awareness - Bullet #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 his daily activities.		2.1.2	
50	E			Situational Awareness - Bullet #4 - Support and participate in statewide information security groups and help to facilitate and leverage the existing communications channels.		2.1.3	

KEY

E,M,N
I,P,D,R
1,2,3

number for reference
E=Existing, M=modified from original, N= new
From NITS - I=Identify, P=protect, D=detect, R=respond or recover
Priority for discussion sake and ordering