Agenda Item # 5

NEVADA CYBERSECURITY PLAN CAPABILITIES ASSESSMENT				FOR ASSESSOR
Cybersecurity Plan Required Elements	Brief Description of Current Capabilities of SLTT within the Eligible Entity	Select capability level from: Foundational Fundamental Intermediary Advanced	Project # (s) (If applicable – as provided in Appendix B)	Met (Yes, No, Partial, or N/A)
1. Manage, monitor, and track information systems, applications, and user accounts				
2. Monitor, audit, and track network traffic and activity				
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts				
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk				
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)				
a. Implement multi-factor authentication				
b. Implement enhanced logging				
c. Data encryption for data at rest and in transit				
d. End use of unsupported/end of life software and hardware that are accessible from the Internet				
e. Prohibit use of known/fixed/default passwords and credentials				
f. Ensure the ability to reconstitute systems (backups)				
g. Migration to the .gov internet domain				
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain				
7. Ensure continuity of operations including by conducting exercises				
8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity)				
9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks				
10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the eligible entity				
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department				
12. Leverage cybersecurity services offered by the Department				
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives				
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats				
15. Ensure rural communities have adequate access to, and participation in plan activities				
16. Distribute funds, items, services, capabilities, or activities to local governments				