Thursday, November 14, 2024
Webinar
9:00 a.m. to noon Mountain Time

Join us for an insightful virtual workshop tailored for low-risk entities. This workshop will provide essential knowledge to small, registered entities on low-impact physical security, Transient Cyber Asset (TCA) and Removable Media (RM), as well as basics of Protection Systems, Automatic Reclosing, and Sudden Pressure Relaying Maintenance. This workshop will not focus on IBRs.

Time	Topics
9:00 a.m.	**Opening Remarks – Steve Noess, WECC**
9:05 a.m.	**Entity Monitoring – Stacia Carron, WECC** Gain an understanding of WECC's monitoring tools (e.g., Compliance Audits, Spot Checks, Self-Certifications) and timelines.
9:15 a.m.	**PRC-005-6 Protection Systems, Automatic Reclosing, and Sudden Pressure Relaying Maintenance Basics — Jessica Molina and Craig Struck, WECC** In this presentation, WECC Compliance Auditors give an overview of the elements of PRC-005-6. We will discuss WECC monitoring approaches and highlight what constitutes a strong Protection System Maintenance Program (PSMP). The purpose of this presentation is to strengthen attendees' knowledge of PRC-005-6 documentation and implementation practices.
10:10 a.m.	**Break**
10:20 a.m.	**Physical Security Best Practices for Low Impact Facilities — Brady Phelps, WECC** In this presentation, WECC's Entity Monitoring Physical Security Lead provides a comprehensive overview of foundational physical security measures for low impact entities. The presentation outlines WECC's audit approach, highlighting key findings from audits and fieldwork to help entities strengthen their physical security controls. The presentation also includes best practices derived from these experiences to foster compliance and enhance security across the region.
11:10 a.m.	**Low Impact Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation — Jennifer Salisbury and Tyler Whiting, WECC** WECC will speak to the effective approaches and methods used for managing Transient Cyber Assets and Removable Media and provide recommendations to strengthen the implementation of cybersecurity plans.
11:55 a.m.	**Adjourn**