Summary of Lessons Learned and FAQs

Table 7 provides a list of the 23 key questions identified during the Implementation Study and whether they are being addressed as an FAQ or lesson learned. Note that all of the questions identified by study participants have been or are being addressed through extensive stakeholder review.

Almost half of these questions relate to CIP-002-5.1 - BES Cyber System Categorization. This underscores an important first step when transitioning to CIP Version 5: responsible entities need to understand the scope of the CIP Version 5 standards and how they apply to the BES Cyber Systems they own or operate.

Table 7: Summary of Key Lessons Learned and FAQs

CIP Version 5 Reference	Description	Degree of Interest by Study Participants	Lesson Learned or FAQ
1. CIP-002-5 R1: Impact rating of generation resources (generation segmentation)	What options are available to categorize the impact rating of BES Cyber Assets at plants greater than 1500 MW?	High	Lesson Learned
2. CIP-002-5 R1: Relay protection in substations with different impact ratings (i.e., far-end relay/transfer trip)	How should the impact rating of line protection relays at each end of a transmission line connecting two substations be determined?	High	Lesson Learned
3. CIP-002-5 R1: Programmable electronic devices	What are some practical examples for what is or is not a programmable electronic device?	High	Lesson Learned
4. CIP-002-5 R1: BES impact of transmission scheduling systems	Should transmission scheduling systems be considered medium- or high-impact rating BES Cyber Systems?	Moderate	Lesson Learned
5. CIP-002-5 R1: Identifying BES Cyber Systems and BES Cyber Assets	What are some practical approaches to identify BES Cyber Systems and BES Cyber Assets?	Moderate	Lesson Learned
6. CIP-002-5 R1: Distributed BES Cyber Assets at generating plants and substations	Are instrumentation devices such as sensors, actuators, and controllers considered to be programmable electronic devices? If so, what methods would be appropriate to secure them from a compliance perspective?	Moderate	Lesson Learned
7. CIP-002-5 R1: Grouping BES Cyber Assets	What are the advantages of grouping BES Cyber Assets into BES Cyber Systems, and how can this help demonstrate compliance?	Moderate	Lesson Learned

Table 7: Summary of Key Lessons Learned and FAQs			
CIP Version 5 Reference	**Description**	**Degree of Interest by Study Participants**	**Lesson Learned or FAQ**
8. CIP-002-5 R1: Shared equipment at a substation	What issues need to be addressed related to substations that are shared by different entities (e.g., identifying ownership, compliance responsibilities, emergency management, physical access controls)?	Moderate	Lesson Learned
9. CIP-002-5 R1: Applicability of Control Centers to Transmission Operators (TOP) and Transmission Owners (TO)	How would CIP-002-5 Attachment 1 criterion 2.12 apply to medium-impact Control Centers if the functional obligations are performed by the TO on behalf of the TOP?	Moderate	Lesson Learned
10. CIP-002-5 R1: Generation interconnection points	Clarify the terms "generation interconnection point," "generation interconnection Facility," and "collector bus" for the purposes of applying CIP-002-5 Attachment 1 impact rating criteria 2.1 and 2.2.	Moderate	Lesson Learned
11. CIP-003-5 R2: Medium-impact rating, non-routable, no dial-up access Cyber Assets	What is the complete set of CIP Version 5 requirements that apply to BES Cyber Systems without routable or dial-up access?	Moderate	Lesson Learned
12. CIP-005-5 R1: Virtual server and network environments	How can virtual environments that physically reside inside and outside an Electronic Security Perimeter be secured and considered compliant?	High	Lesson Learned
13. CIP-002-5 R1.2: Serial devices with External Routable Connectivity	Are serial based systems with local serial connections considered to have External Routable Connectivity if they are remotely accessible via routable protocol?	Moderate	Lesson Learned
14. CIP-005-5 R1.5: Intrusion detection systems	Discuss the merits of installing intrusion detection systems outside the Electronic Security Perimeter.	Moderate	Lesson Learned
15. CIP-005-5 R2: Interactive remote access	What needs to be considered to determine if an electronic connection is Interactive Remote Access?	Moderate	Lesson Learned
16. CIP-005-4: Electronic Access Monitoring and Control Systems	How should mixed-trust authentication processes (e.g., corporate active directory systems that authenticate access to an energy management system) be managed to ensure compliance?	Moderate	Lesson Learned

Table 7: Summary of Key Lessons Learned and FAQs			
CIP Version 5 Reference	**Description**	**Degree of Interest by Study Participants**	**Lesson Learned or FAQ**
17. CIP-006-5 R1: Multiple physical access controls	Discuss options for using two or more physical access controls for high-impact BES Cyber System Physical Security Perimeters.	Moderate	FAQ
18. CIP-007-5 R1: Protecting physical ports	How can tamper tape be used to protect physical ports to comply with this requirement?	Moderate	FAQ
19. CIP-007-5 R2: Identifying sources for patch management	How should the appropriate sources for obtaining security patches be determined and documented?	Moderate	FAQ
20. CIP-007-5 R3.2: Mitigate the threat of detected malicious code	Clarify if entities are required to mitigate the threat of detected malicious code regardless of the methods they choose to deter, detect, or prevent malicious code.	Moderate	FAQ
21. CIP-010-2 R1: Change management	What are some methods to automate the change and configuration management process for substation equipment?	Moderate	Lesson Learned
22. CIP-010-2 R3: Vulnerability testing of Physical Access Control Systems	How should active vulnerability scans be managed for Physical Access Control Systems given their sensitivity to denial of service attacks?	Moderate	FAQ
23. CIP-010-2 R4: Protection of transient devices	What are the protection requirements for transient devices used for maintenance activities?	Moderate	FAQ