1. Would event-triggered cybersecurity supply chain risk assessments performed for a product or service reset the 24- or 36-calendar month clock for R1.3 for that product or service?

   Yes. As stated in the requirement, the 24 or 36-calendar month period is measured from the last completed risk assessment performed pursuant to the entity's SCRM plan(s); this holds irrespective of whether the risk assessment was triggered by an event or was performed under R1.1, R1.3, or R1.4.

2. Would event-triggered cybersecurity supply chain risk assessments performed for a vendor, product or service reset the clock for the periodic assessment required by R1.4?

   Yes, if that is what is stipulated in the entity's SCRM plan(s). Cybersecurity supply chain risk assessments for a particular vendor, product or service performed pursuant to the entity's SCRM plan(s) would reset the R1.4 clock for that vendor, product or service.

3. Why does R1.3 establish a period in which the assessment must be performed, but R1.4 does not?

   FERC Order 912, paragraph 26-1 directed the establishment of a maximum timeframe between the initial risk assessment and deployment of the product or service. This is reflected in R1.3. Concerning R1.4, the Order did not mandate the establishment of a specific periodicity for risk reassessment post-deployment. It is instead left to the entity to document in their SCRM plan(s) what that periodicity should be. Periodicities can vary based on service or device type, impact rating, implementation of continuous monitoring, or other factors as explained in the CIP-013-4 Technical Rationale.

4. If an entity were to procure N of the exact same product, a reassessment of the product performed under the SCRM plan(s) would cover the entity for all instances of that particular product (i.e. assets) until the R1.4 periodic reassessment interval is reached. Is this an accurate statement?

   Yes. The assessment is of the ***product***, not the asset. For example, entity X procures 10 of microprocessor relay product Y, all of which have the same hardware and firmware version. The assessment of relay product Y covers the entity for all instances (e.g. the primary or secondary line relays) of that product in entity X's CIP-013 R1 applicable systems (e.g. the protection systems for BES transmission feeders 1, 2 and 3).

5. Why are entities required to periodically reassess assets, if those assets are already required to undergo the CIP-010 vulnerability assessments on a periodic basis?

   The CIP-010 vulnerability assessments are performed to assess the risks associated with specific assets and systems, in accordance with the Responsible Entity's vulnerability assessment program(s). The assessments described in CIP-013 in contrast aim to identify and address risks associated with vendors, products and services (not assets and

systems). Moreover, supply chain risks are fundamentally different than the types of risks identified through a vulnerability assessment. Lastly, periodic supply chain risk reassessments were explicitly directed by FERC in paragraph 26-2 of Order 912.

6. Are products procured prior to the effective date of CIP-013-1 subject to R1.4?

   Yes. The FERC Order does not carve any exclusions for products. Any product included in a CIP-013 R1 applicable system is subject to the requirement. This includes but is not limited to products that are considered end of life (EOL) or end of support (EOS). EOL/EOS products may pose risks due to the lack of production of spares and replacements, as well as the loss of support, including but not limited to troubleshooting and availability of patches to address discovered vulnerabilities. As part of the supply chain risk assessment process, entities should identify the risks posed by the continued use of the products in their environments and the risk management strategies they plan to use to address them.

7. Are vendors that did, but do not currently have an active contract with the Responsible Entity, subject to the R1.4 periodic risk reassessment?

   Assessing vendors that do not have an active relationship with the entity (e.g. finalized or planned agreements pertaining to procurement, maintenance, support, etc.) would not seem to provide a discernable benefit to reliability. In certain cases, however, it may be prudent to assess these vendors, even if they do not have an active contract with the entity. A vendor, for example, may publish security patches that are freely available to anyone using their software, irrespective of whether the user of the software has an active support agreement in place with the vendor. The SDT recommends that entities define in the SCRM plan(s) one or more criteria to determine whether a vendor should undergo periodic reassessment.

8. How should entities assess vendors that no longer exist?

   Entities should handle this eventuality in accordance with their SCRM plan(s). For example, if the vendor were acquired by another company, the entity can assess the acquiring entity in lieu of the acquiree. If the vendor were to cease operations entirely, they would fall out of scope for the reassessment requirement. Any products procured from that vendor that are present in or are destined for a CIP-013 R1 applicable system, however, would still be subject to the requirements in the Standard.

9. If a system is reclassified to an R1-applicable system after it has been procured and deployed (e.g. the system impact rating increased from Low to Medium due to a new interconnection), how would an entity demonstrate compliance with R1.1 through R1.3?

   In this scenario, the entity should be prepared to demonstrate that the sub-requirements were not applicable to the reclassified system at the time of procurement (R1.1, R1.2) and

deployment (R1.3). The reclassified system would be subject to the R1.4 periodic assessment requirement post-reclassification.

10. Are PCAs procured prior to the effective date of CIP-013-4 subject to R1.1?

    No. Per the Project 2025-06 Implementation Plan, entities are not required to perform retroactive R1.1 assessments for PCAs procured prior to the effective date of CIP-013-4.