

PRELIMINARY SED Recommendation on Utility Straw Proposal Scope, September 29, 2017

Security plans, independent review, and regulatory-oversight body adoption. The Utilities' straw proposal is expected to ultimately commit each utility to a multi-step security-resiliency demonstration-of-compliance process for distribution infrastructure not subject to NERC CIP-014.

SED recommends the following six-step procedure for onboarding of a physical security mitigation plan ("security plan" or "plan") to address utilities' distribution assets. The proposed six steps are modeled on security plan requirements prescribed by NERC CIP-014.

- Step 1. Assessment. Drafting of a plan, addressing prevention, response, and recovery, which could be prepared in-house or by a consultant.
- Step 2. Independent Review and Utility Response to Recommendations. Proposed plan would be "reviewed" and deemed appropriate and adequate by some independent third party, likely a qualified consultant expert, national laboratory, or a regulatory or industry standard body (such as the Electric Power Research Institute. Step 2 would include reviewer recommendations, including mitigation measures. Utilities would be expected to fully address reviewer recommendations, including justifying any mitigations that it declines to accept; this utility response, in concert with threat and risk assessment, and mitigation measures together would constitute a final plan report.
- Step 3. Validation (for IOUs only). Final plan report would be validated (recurring every five years)¹ so as to deem it adequate, in compliance, and eligible to request funding for implementation.² The validation would be performed by the CPUC Safety and Enforcement Division (SED). Non-compliance may be met with a violation order to be followed up with sanctions and/or penalties by SED.
- Step 3a. Validation (for POUs only). Final plan report would be validated by a qualified authority designated by the applicable local governance body. (The Riverside example of a POU plan conforming to CalOES and FEMA standards and receiving their endorsement would be one example of an acceptable approach.)
- Step 4. Adoption. Validated plan would be submitted to the appropriate regulatory oversight body (for IOUs, the CPUC; for POUs, their local governance body) for review and greenlighting (adoption). Step 4 should include funding to implement the plan.
- Step 4a. (for POUs only). Notice. Provide CPUC with official notice (ideally including a copy of a resolution) of the adopted plan action.
- Step 5. Maintenance. Ongoing adopted plan refinement and updates as appropriate and as necessary to preserve plan integrity. All security plans should be concurrent with and integrated into utility resiliency plans and activities.
- Step 6. Repeat Process. Plan overhaul and new validation after five years.

¹ This time interval is based on the requirements instituted for the City of Los Angeles under City Charter.

² Upon five years from the date of adoption, a utility would be required to have any revised or original plan updated and repeat the validation process. Utilities would be afforded regulatory relief by way of an exception request process for special cases where undertaking of the plan overhaul and/or validation processes may be impracticable or unduly burdensome.