1. Substation located in Alamogordo, NM has a broken fence.
2. Firewalls improperly configured.
3. Username and password buffer overflow was discovered in a web-based Human Machine Interface (HMI) Web server.
4. Data transfer from the Operational Technology (OT) side to the Information Technology (IT) side of the Enterprise network is unencrypted.
5. Systems remain unpatched until after a year when the patch became available.
6. Rogue WiFi Access Points (APs) were discovered within the company premises.
7. Improper network segmentation between the IT and OT sides of the Enterprise.
8. Unused opened ports were discovered in the Data Historian server.
9. Insufficient disaster recovery preparation.
10. Lack of lockout system enforcement for failed login attempts.
11. Lack of separation of duties through assigned access authorization.
12. Insufficient cyber security policies.
13. The non-employee entered the OC premises by tailgating.
14. There is no documented process for employee termination.
15. Remote access to the OT equipment and systems is not secure.
16. Company equipment is allowed to be carried outside of company premises.
17. Some substations are not secured.
18. Security awareness training for employees is outdated and nonperiodic.
19. The IR plan has not been reviewed and updated for 5 years.
20. The access control mechanism on the Historian is extremely weak.
21. The HMI server has not been patched—missing at least 3 full patch versions.
22. The testing procedure for the Cybersecurity Recovery Plan is not documented.
23. Vulnerability assessment on both IT and OT systems is outdated.
24. There is no documented process on vetting equipment vendors.
25. Computing equipment and storage devices are being donated to non-profit organizations without data sanitization.