Good afternoon, (Power company executive) this message is sent to you regarding your request about vulnerability management and finding a suitable process for vulnerability management. First off, vulnerability management is a process that can be included in IT environments or systems with the goal of making the system more secure. Things that help achieve this in vulnerability management would be things like a vulnerability assessment, security configuration management and compliance, IT security risk management, and security information and event management.

Your company needs vulnerability management because while vulnerabilities may not be at the same severity level as a breach or attack however vulnerabilities are what lead to breaches and attacks. While being an electric power company your power grids are essential to many American lives and as such is why it demands a high level of availability to make sure Americans get the power, they need for their day to day lives as well as the integrity to uphold their data safely and protect the power grid and concurrent systems properly. By incorporating the proper vulnerability management your electric company and systems will be able to further protect and provide to your customers. One example of how vulnerability management could help your company would be let's say your vulnerability scanner picks up on a not yet updated patch that fixes a huge bug on windows systems that allows hackers to gain admin privileges. Stopping a serious potential attack by just updating software. Helping aid in the preventing attacks against your systems before they start.

The typical process of vulnerability management can be categorized into six categories being asset inventory management, information management, risk assessment, vulnerability assessment, reporting and remediation tracking, and response planning. An asset inventory is essential to properly identifying what security alerts are associated with what assets and who,

what, where that asset was last is or is located. Some tools to help achieve this are provided by LANDesk. Information management uses a Computer Security response team to identify and work on which vulnerabilities are the most serious at the current moment and manages the flow of new information into the organization. Risk assessments should be conducted regularly to preserve confidentiality, integrity, and availability of all IoT assets. A tool to help with risk assessments would be ArcSight. Vulnerability assessments will be used to find which assets are the most vulnerable with things like Nmap and Nessus. Reporting and remediation tracking is the process of documenting the full process of vulnerability to patch to ensure it is taken care of. Finally, a response plan should be put in place to in depth detail what all personnel should be doing in the event of a new vulnerability.

Additional personnel may be needed for many roles to help support all this new framework and policies in vulnerability management. Some positions being:

- Chief Information Security Officer (CISO) or IT security Manager
- Network and Systems Administrators
- Risk and Compliance Managers
- Vulnerability Management analyst

Including vulnerability management into your company's framework is a critical component needed for electric power companies trying to face the ever growing and ever-increasing cyber threats targeting critical infrastructure industries. By implementing a solid vulnerability management process your power company can improve their resilience to cyber-attacks and protect critical assets.