**Scenario:**
You are a cybersecurity analyst on the security team at Red Cell 637 Defense, a DoD contractor specializing in cyber operations and defensive strategies.

High-ranking federal government officials informed your team that recent intelligence shows an advanced persistent threat (APT) is looking at exploiting supply chain vulnerabilities against the computers that operate the Western Interconnection power grid. You are to assume that this APT originates from either a well-funded nation state or terrorist group. The APT has been able to probe and map the network over the course of several months. The officials have given your team access to classified intelligence indicating that the currently unidentified group may be planning to install malicious malware within the grid’s computer network that will disrupt power to eleven states.

Your team has been asked to work closely with the DoD, Department of Homeland Security (DHS), and other federal stakeholders to strengthen the security and safety of the power grid and its related computer information systems.

The DoD regards mission assurance as the ability to provide continuous operations despite attacks, system failures, or other disruptions. Mission assurance is a vital part of maintaining critical infrastructure protection. The final component of your plan is to develop protection and detection recommendations to secure against future cyber threats to the critical infrastructure services of the Western Interconnection power grid. You will need to clearly explain the safeguards you have selected, providing explicit detail (e.g., graphics, references) to ensure your recommendations are clear. You will explain how applying these safeguards considers the future role of cyberwarfare.

**Requirements:**

*Your submission must be your original work. No more than a combined total of 30% of the submission and no more than a 10% match to any one individual source can be directly quoted or closely paraphrased from sources, even if cited correctly. Use the Turnitin Originality Report available in Taskstream as a guide for this measure of originality.*

*You must use the rubric to direct the creation of your submission because it provides detailed criteria that will be used to evaluate your work. Each requirement below may be evaluated by more than one rubric aspect. The rubric aspect titles may contain hyperlinks to relevant portions of the course.*

A.  Recommend specific safeguards to protect the delivery of critical infrastructure services at the Western Interconnection power grid. Be sure to explain how these recommended safeguards will protect the critical infrastructure services.

B.  Describe how each safeguard you recommended would need to change over time with the evolution of cyber-related capabilities, changing threats, and emerging technologies.

C.  Recommend functions or systems that would enable the timely detection of cybersecurity threats. Be sure to explain how each function or system would detect cybersecurity threats.

D.  Describe how each function or system you recommended would need to change over time with the evolution of cyber-related capabilities, changing threats, and emerging technologies.