BISF ASSIGNMENT 1 & 2

In critical infrastructure security, all standards organizations, regulations, and recommendations indicate that a defense-in-depth strategy should be implemented.

i) Map out a Defense in Depth Perimeter you would apply in strategizing the security of a critical infrastructure component along with the Corresponding Protective Measures.

Physical security:

- Installation of a heavy-duty perimeter fence is put up to establish a strong barrier for ensuring security on the vital infrastructure.
- Preventive and detective control like CCTV cameras on the infrastructure inside and outside the building, for monitoring the perimeter
- Implement physical control access to the building .like, electric doors where authorized personnel can access using the codes, use of biometric scanners or use of access cards.

Information Security:

- Establish policies that protect the information- Limit access of individual or employees that have entry to the most sensitive information of the infrastructure.
  -Implement password policy, like password management softwares that can auto-generate password that will meet required guidelines. Also, use multi-factor authentication for user or staff verification.
- Secure Data storage- strategies to protect all data storage both physical and non-physical. Solutions like encryption, access control and recovery strategies e.g. backup and disaster.
- Educating and creating awareness to the staff about data protection and best practices for it

Network Security:

- Strategies of the network security include -implementing firewalls to control incoming and outgoing network traffic.
  -Intrusion Detection and Prevent Systems this systems help monitor network traffic for suspicious activity.
  -Virtual Private Networks for safe remote network access.
- Network monitoring and Logging for anomalies and monitor unauthorized access
- For the Wireless Network Security I would segment the wireless traffic from the main network and also use strong encryption.

Cloud Security:

- Logging and monitoring to make sure the rules are followed and standard to find weakness and vulnerabilities.
- Ensure a trustworthy cloud provider that can take security responsibilities.
- Control measures, for who can access what is crucial, to make sure sensitive data remains encrypted.

Incident Response and Management:

- Its designed to efficient manages and reduce incidents that arise in an essential infrastructure element.
- Develop a plan - an Incident Response Plan that will give guidelines on how to identify report and respond to an incident of security.
  -Recovery Plan is strategy for recovering the affected systems during an incident. Implement preventive measure to prevent a similar incident from happening and various ways to improve the security and reduce vulnerabilities.
  -Regular training for a team created to respond to such incidents to ensure they are all prepared to respond effectively in real-life situations