**A. WLAN Vulnerabilities**

**1A. Signal being accessed beyond the intended premise vulnerability.**

The WLAN Access Point servicing the back patio could potentially have a signal range that extends beyond the company premises, making it susceptible to unauthorized access.

**1B. Insecure remote access to website server.**

The second WLAN vulnerability pertains to potentially insecure remote access to Alliah's website servers, located 100 miles away from the headquarters. If the IT staff is using unsecured or weakly secured methods to remotely access these servers, the company risks unauthorized access or data breaches.

**B Mobile Vulnerabilities**

**1B. BYOD Policy Vulnerability**

The Bring Your Own Device (BYOD) policy exposes the network to a wide variety of security configurations and potential vulnerabilities, particularly malware infections and data leakage.

**2B. Remote Work Vulnerability**

Account representatives often work remotely, potentially connecting to insecure networks and thereby exposing sensitive data to risk.

**C. Mitigation**

**1C. Mitigation for Signal being accessed beyond premises WLAN**

Conduct a wireless site survey using a Wireless Site Survey Tool to map the reach of the WLAN, especially the access point servicing the back patio. If the signal reaches beyond the building, adjust the power levels of the wireless access points.

Tools Needed: Wireless Site Survey Tool

*(NIST Special Publication 800-48)*

**2C. Mitigation for Insecure remote access to web servers.**

To mitigate this risk, it's essential to implement a Virtual Private Network (VPN) solution for secure and encrypted connections between the IT staff at the headquarters and the remote servers. Multifactor authentication (MFA) should be added to ensure that only authorized personnel can access the remote servers. This will significantly enhance the security of remote access to Alliah's servers.

Tools Needed: VPN tool MFA

*(NIST SP 800-77)*

**C1. BYOD Policy Mitigation for Mobile devices**

Deploy a Mobile Device Management (MDM) solution. Enforce security policies such as encryption, screen locks, and remote wipe on all BYOD devices through the MDM. Regularly audit the devices for compliance.

Tools Needed: MDM Solution

*(FISMA guidelines for mobile security)*

**C2. Remote Work Mitigation for Mobile devices**

Procure a Virtual Private Network (VPN) solution for the company. Configure VPN settings to require end-to-end encryption. Mandate the use of the VPN for all remote work.

Tools Needed: VPN Service

*(NIST SP 800-77)*

**D. Preventative Measures**

**In this section, you need to list preventive measures that will increase the security posture of the WLAN and mobile environment. You need to list a preventative measure for EACH**

**Preventative Measure for WLAN**

Implement Multi-Factor Authentication for gaining access to the WLAN. This ensures that users will need more than just a password to access the network, making it much more challenging for unauthorized persons to gain access.

**Preventative Measure for Mobile environment**

Implement data masking and encryption features on all mobile devices that store or have access to company-sensitive data, especially Personally Identifiable Information (PII). This ensures that in case a device is lost or stolen, the data remains inaccessible.

**Reference federal, state, or industry regulations that justify these measures.**

*The Sarbanes-Oxley Act (SOX)* places heavy emphasis on the integrity of financial data and systems that store this data. With Alliah's ambition of potentially going public, implementing MFA can ensure compliance with SOX requirements.

*General Data Protection Regulation (GDPR)* heavily regulate the protection of PII. Data masking and encryption ensure that Alliah is in compliance with these regulations.

**E. Recommended BYOD Approach**

**First Recommendation: Containerization of Corporate Data on Personal Devices**

This approach involves segregating business and personal data on an employee's personal device. Through containerization, a virtual boundary is set up on the device that keeps corporate data separate and secure. This way, even if the personal side of the device is compromised, the corporate data remains secure. *(NIST 1800-22)*

**Second Recommendation: Endpoint Security Management**

This involves the use of an endpoint security management system that can remotely manage, lock, or wipe the corporate data in case the device is lost or stolen. This gives the organization control over the data without controlling the entire device.*(NIST 1800-22)*