Oregon
Tina Kotek, Governor

Enterprise Information Services
Cyber Security Services
550 Airport Rd SE
Salem, OR 97301
PHONE: 503-507-2678

MEMORANDUM

To: All Agency Directors

CC: All Agency Chief Information Officers

From: Ben Gherezgiher, Chief Information Security Officer B.G.

Date: October 28, 2024

Subject: Cyber Security Services Directive: Strengthening Cybersecurity of the State Enterprise

As the working environment for the State of Oregon has changed dramatically in recent years, the State of Oregon enterprise requires robust, unified solutions to provide for the protection, detection, and response capabilities to meet the demands of a distributed workforce. Siloed systems are often disparate and discordant, which inhibits the ability to protect, monitor, detect, and correlate threat activity throughout the enterprise.

Keeping in line with the State Chief Information Officer's Strategic Framework, version 2.0, EIS has invested in technologies to provide for the protection, detection, and response capabilities that will help implement enterprise-wide safeguards, accelerate notification of cyber threats, and consistently respond to anomalies and suspected events. Cyber Security Teams are directing mitigation actions in line with that framework, and its objective, to improve Oregon's cybersecurity posture.

These actions support the fundamental pillars of cybersecurity in an enterprise and serve as the first line of defense against cyber threats. Additionally, the enterprise can mitigate the impact of cyber-attacks, reduce the time to respond, and prevent further compromise of sensitive data.

With the help of state agencies, boards, and commissions (hereafter known as state agencies), two major efforts have been underway to better position the enterprise in achieving these capabilities:

1) The Microsoft Security Enhancement project has an initiative to hybrid-join all Windows desktops to Entra ID (formerly known as Azure Active Directory "AAD"). Hybrid-joining machines, which connect to both Azure Active Directory (AAD) and on-premises Active Directory, offer several benefits:

    a. Single Sign-On (SSO): Users can seamlessly access both on-premises and cloud resources without needing separate logins.
    b. Improved Security: Enables conditional access policies, multi-factor authentication, and modern identity security.
    c. Centralized Management: Facilitates management of devices across both cloud and on-premises environments through tools like Microsoft Endpoint Manager.
    d. Transition to Cloud: Provides a smoother migration path to cloud services while retaining access to legacy systems.

2) Onboarding systems with the Microsoft Defender suite (e.g. Defender for Endpoint, Defender for Cloud, Defender for Identity) to unify security event telemetry into the Microsoft security portal and enterprise Microsoft Sentinel Security Information and Event Monitoring (SIEM) for better proactive monitoring and tracking of security related issues.

The time to close these cybersecurity gaps is now, as the enterprise increasingly faces sophisticated cyber threats that exploit vulnerabilities in outdated systems, unprotected networks, and inadequate defenses. With the rise in ransomware attacks, data breaches, and phishing campaigns, proactive measures are essential to safeguard digital assets.

By fully implementing these initiatives, the enterprise can significantly reduce risk. Addressing these gaps promptly is critical to protecting sensitive information, ensuring business continuity, and maintaining trust with our constituents in an interconnected world.

Effective immediately, the following requirements are mandatory for all state agencies under the authority of ORS 276A.300:

1) All Windows systems must be hybrid-joined to Entra ID.
2) All systems (Microsoft, Linux, and MacOS) must be onboarded with Microsoft Defender and ensure they are being monitored through the enterprise Cyber Security Services Security Operations Center (CSS SOC).
3) Defender for Identity must be installed on all domain controllers.
4) Defender Antivirus is the standard anti-virus/anti-malware solution and must be installed, operational and kept updated. As part of the Microsoft M365 G5 licensing procurement, all state agencies are licensed to use Microsoft Defender Antivirus on all systems – at no additional cost. State agencies must begin the process of installing Microsoft Defender Antivirus and setting it to 'active mode'. This transition is not expected to last beyond 90 days from the date of this memorandum.
5) Defender Network Protection must be enabled.
6) Agencies to enroll endpoints in MS Intune for visibility and security monitoring.

Agencies unable to fully comply with these requirements must notify CSS by November 28, 2024. CSS will provide guidance and support to establish a plan for reaching compliance. If you need assistance, please contact the CSS SOC at css-soc-services@das.oregon.gov.

Thank you for your support and assistance in sponsoring this important initiative to enhance our cybersecurity defenses.