Microsoft Federal

Federal Agencies Partner with Microsoft to **Meet Cybersecurity Executive Order Milestones**

THE CYBERSECURITY EO AT A GLANCE

The United States is facing increasing cyber attacks that threaten critical infrastructure, and the security and privacy of the American people. We need a concerted, national response that brings together the Federal Government and leading private sector companies to protect the nation from malicious cyber actors.

On May 12, 2021, the Biden Administration signed an Executive Order on Improving the Nation's Cybersecurity that represents a bold step in recognizing cybersecurity as a national priority and provides concrete recommendations to address ever-evolving and increasingly sophisticated threats. The purpose of the EO is to modernize the government's IT infrastructure with a set of standards that will enable them to be more proactive when dealing with cyber threats. For federal agencies, there are numerous short-term deadlines and requirements highlighted in the EO that must be met in the next few weeks and months. These deadlines should not be viewed as a 'check-the-box' compliance effort; rather, they are meant to improve the overall security posture of the Federal Government and should fit within an agency's long-term security strategy.

KEY EO MILESTONES

2021

July 11, 2021: Agencies must update plans for federal network infrastructure including adoption of cloud technology and implementation of Zero Trust Architecture and report their plans to OMB/NSC.

July 26, 2021: Agencies must establish a MOA with CISA for Continuous Diagnostics and Mitigation 'CDM' and ensure CISA has access to object level data.

August 10, 2021: Heads of federal civilian agencies must evaluate and classify agency data and provide a report of this evaluation to DHS and OMB.

Agencies must comply with NIST/CISA/OMB guidance on security measures for critical software including applying practices of least privilege, network segmentation, and proper configuration.

August 24, 2021: Agencies must establish requirements for logging, log retention, and log management which will ensure centralized access and visibility for the highest level security operations center of each agency.

September 9, 2021: Federal civilian agencies must adopt government-wide EDR approaches based on OMB requirements.

November 8, 2021: Agencies must adopt MFA and encryption at rest and in transit, to the maximum extent, and report on progress every 60 days.

2022

March 8, 2022: Agencies must comply with the guidance identifying practices that enhance the security of the software supply chain with respect to software procurement.

HOW FEDERAL AGENCIES CAN ACCELERATE MODERNIZATION AND MEET EO MILESTONES

While the timelines established by the EO's mandate seem aggressive, they are also very attainable. Strengthening our nation's cybersecurity is achievable through close collaboration between government and industry, leveraging modern cybersecurity strategies across the entire digital ecosystem.

The hard work of IT modernization is already underway and much of the groundwork for supporting the EO has been laid. In fact, many agencies may not realize they already have technology in place that simply needs to be activated or fine-tuned to meet the EO requirements. By tapping into technology they already have, Federal CIOs and CISOs can save significant time and cost as they navigate near- and long-term modernization strategies.

For the first time ever, the EO acknowledges cloud as the secure path to building out a holistic security strategy. With centralized cloud solutions, Microsoft has always been at the forefront of innovation and stands ready to help agencies meet the requirements stated in the cyber EO. Microsoft is fully aligned with agency needs offering a cloud that directly addresses zero trust, cloud adoption and modernization, data discovery, classification and protection, multi-factor authentication and encryption and endpoint detection and response. We look at our strategy as part of a journey from the implementation of zero trust all the way through each EO milestone and beyond.

To guide agencies, Microsoft's Cloud Adoption Framework provides a rich repository of documentation, implementation guidance, and best practices to help accelerate the cloud adoption journey. Resources and roadmaps like our rapid modernization plan (RAMP) and Zero Trust Architecture plans simplify the complex to ensure strategies are successfully integrated, while teams like FastTrack can help agencies plan and address change quickly and effectively. Utilizing these resources will help agencies meet aggressive EO timelines and achieve a hardened cybersecurity posture.

MICROSOFT HAS OUTLINED A FEW IMMEDIATE STEPS AGENCIES CAN TAKE TO MEET THESE IMPORTANT CYBER EO MILESTONES:

STEP ONE
To identify and monitor risks, agencies should enable single sign-on to applications, set up conditional access to enforce MFA, and register and provision devices to establish a dynamic asset inventory. They should implement identity solutions that they already own, like Azure Active Directory 'AD' single sign-on, and Azure Active Directory's Application Proxy, which provides secure remote access to on-premises web applications.

STEP TWO
To establish risk-prioritized actions, agencies should use a cloud-native, security information event management 'SIEM' and security orchestration automated response 'SOAR' solution like Azure Sentinel that provides additional insights through anomaly detection. Many agencies already have the capability to identify sensitive information in Office 365 and on-premises with Microsoft Information Protection. Using Azure Virtual Desktop for remote administration via cloud SAW and segmenting privilege with cloud-only administrator accounts are also easy steps that significantly reduce risk.

STEP THREE
To increase cyber protections, agencies should enforce BYOD mobile device management 'MDM' enrollment during authorization to provide an inventory of non-enteprise devices, proactively manage updates, patches, policies, and device health, and enable endpoint detection and response. Solutions like Azure Defender and Microsoft Cloud App Security provide deeper analytics and fine-grained control so agencies can gain greater visibility into cloud apps and services to control sessions and protect workloads in real-time

DELIVERING TRUST AT SCALE TO IMPROVE NATIONAL SECURITY

As federal agencies forge ahead in a changed world, they can turn to Microsoft's transformative cloud as the engine for innovation, efficiency, a new way to work and delivering trust at scale. Microsoft Federal is here to help the government answer the nation's call on strengthening inter- and intra-agency capabilities to unlock the government's full cyber capabilities. Our unique approach is built on the decades of trust we've earned in helping our federal customers achieve their mission. We thoroughly understand both the landscape in which agencies operate and this current challenge, and we know how to collaboratively build the roadmap for continuous improvement. Together, Microsoft Federal can help agencies not just reach modernization milestones but achieve greater collaboration and trust — so we can protect what matters most.

Microsoft Federal