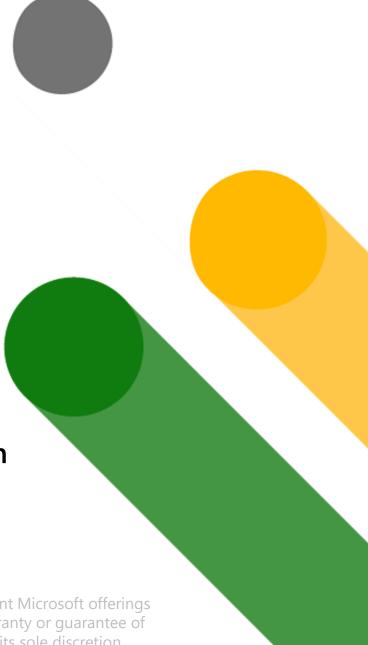


## Executive order on improving the nation's cybersecurity

**Microsoft Federal Resources** 

Federal Zero Trust modernization plan



## Zero Trust phased rollout plan to accelerate modernization

Phase 1: Identify and monitor	Phase 2: Reduce risk	Phase 3: Increase protection
<ul> <li>Enable single sign-on to applications</li> <li>Set up Conditional Access to enforce MFA</li> <li>Register devices and remotely provision and deploy new devices</li> </ul>	<ul> <li>Enable Risk-based Conditional Access</li> <li>Enable Identity Protection</li> <li>Enforce cloud-only dedicated cloud administration accounts</li> </ul>	<ul> <li>Enforce BYOD MDM enrollment</li> <li>Proactively manage updates, patching, policies and monitor device health</li> <li>Enable endpoint detection and response with Microsoft Defender for Endpoint</li> </ul>
<ul> <li>Connect on-premises infrastructure to cloud</li> <li>Every workload is assigned an app identity</li> <li>Establish and monitor micro-perimeters with landing zones and Azure Firewall</li> <li>Monitor cloud security posture with ASC</li> </ul>	<ul> <li>Deploy Azure virtual desktops SAW and restrict server management with Azure Arc DSC for hybrid micro-segmentation</li> <li>Enable network and infrastructure anomaly detection with Azure Sentinel</li> </ul>	<ul> <li>Control session with MCAS app protection</li> <li>Protect workloads with Azure Defender</li> <li>Enforce additional micro-segmentation with Azure Policy and Network Security Groups/Application Security Groups</li> </ul>
<ul> <li>Use Azure AD SSO for cloud apps</li> <li>Use Azure AD App Proxy to enable access to on-premises web apps</li> </ul>	<ul> <li>Define Sensitive data types and enable automated labeling</li> <li>Monitor aggregate sensitive data flows</li> </ul>	<ul> <li>Enforce data and application access policies</li> <li>Enable Information Protection policies</li> <li>Utilize Information Protection ML classifiers for custom detections</li> </ul>