Microsoft Security

# Executive order on improving the nation's cybersecurity

## Microsoft Federal Resources

## Federal Zero Trust modernization plan

The information in these slides represent current Microsoft offerings and solutions and are offered without any warranty or guarantee of any kind and may be changed by Microsoft at its sole discretion.

# Zero Trust phased rollout plan to accelerate modernization

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