TALKING POINTS
Zero Trust Principles to Federal Enterprise Mobility

LAST UPDATED: 3.7.2022

***REMINDER:** These talking points are "For Official Use Only" for staff who are acting in an official capacity. These talking points are NOT intended for media engagement. Please contact cisamedia@cisa.dhs.gov with any media inquiries.*

ZERO TRUST PRINCIPLES TO FEDERAL ENTERPRISE MOBILITY BACKGROUND AND TALKING POINTS

BACKGROUND

The Cybersecurity and Infrastructure Security Agency (CISA) has published new guidance for Federal agencies as they evolve and operationalize cybersecurity programs and capabilities, including cybersecurity for mobility. The new guide, "Applying Zero Trust Principles to Enterprise Mobility," is intended to inform agencies about how zero trust principles can be applied to currently available mobile security technologies that are likely already part of a federal enterprise's mobility program.

KEY MESSAGES

- As America's cyber defense agency, CISA published *Applying Zero Trust Principles to Enterprise Mobility* on March 7, 2022. The paper is intended to guide federal civilian agencies and other organizations through the process of developing and implementing their specific cybersecurity capabilities for enterprise mobility toward adoption of their ZT goals.
- Mobile devices present unique opportunities and challenges in adopting comprehensive zero trust models. We understand that mobile devices are an integral resource to conducting official business. This new publication highlights the need for special consideration for mobile devices and associated enterprise security management capabilities due to their technological evolution and ubiquitous use.
- The new guidance presents architectural frameworks, principles, and capabilities to attain a ZT level set by the adopting organization. It then maps mobile security approaches into ZT principles that an organization can use to align its current mobile security capabilities with a ZT approach.
- This guidance was developed through an interagency effort called the Federal Interagency Mobility Group, which was established as part of the Federal CIO Council. It is meant to be a complimentary effort to the recently released OMB Zero Trust Implementation Template and CISA Zero Trust Maturity Model.
- CISA is requesting public comment to ensure our guidance enables the best visibility, flexibility, and security. Our intent is to inform federal agencies how ZT principles can be applied to currently-available mobile security technologies that are already adopted in many cases as part of enterprise mobility security programs.

TALKING POINTS

What is this new guidance:

The Cybersecurity and Infrastructure Security Agency (CISA) published new guidance for federal agencies and other organizations to us as they evolve and operationalize cybersecurity programs and capabilities to include cybersecurity for mobility.

- "Applying Zero Trust Principles to Enterprise Mobility" informs agencies about how zero trust (ZT) principles can be applied to currently available mobile security technologies that are likely already part of a federal enterprise's

mobility program.

- It is written to guide federal civilian agencies and other organizations through the process of developing and implementing their specific cybersecurity capabilities for enterprise mobility toward adoption of their ZT goals.
- Until April 20, 2022, CISA invites all stakeholder and partners to review and provide comments that can help ensure our guidance enables the best visibility, flexibility, and security.

Why was this guidance written:

While key federal government documents on Zero Trust approaches provide broad perspectives, a review revealed that the mobile device is treated as another end-point device.

- This new guidance highlights a need for special consideration for mobile devices and associated enterprise security management capabilities due to their technological evolution and ubiquitous use.
- It is expected that the mapping presented in this guidance will help in the adaptation or development of an enterprise-wide mobile security program that aligns with organizational ZT objectives.
- It is important to note that the mobility ZT paper is not a technical manual or implementation guide for either zero trust or enterprise mobility – it is a guide.

Additional details:

In addition to the zero trust mapping tables, this new resource provides proposed next steps for agencies, which can also be helpful to non-federal organizations, such as:

- Organizations should develop a strategy and their own ZT roadmap consistent with their mission and business needs and in response to OMB's ZT strategy and timeline.
- Organizations should conduct risk assessments against organization specific ZT goals to develop formalized approaches for technical changes as well as personnel policies and processes for the mitigation of residual risks.
- Organizational policies should specify granularity of continuous authentication and standards for mobile device health assessments.

FOR MORE INFORMATION

To learn more about the Zero Trust Principles to Federal Enterprise Mobility please visit CISA.gov. For more information or for additional help, contact CISA-ExternalAffairs@hq.dhs.gov. For media inquiries, please contact CISA Media at CISAMedia@cisa.dhs.gov