

CISA Zero Trust Model

Executive Summary for Agency Leadership

Prepared by: Tim OHagan
Date: Nov 29, 2024

DATA SOCIETY

Executive Overview

The federal government is modernizing its cybersecurity approach. CISA's Zero Trust Model mandates a shift from perimeter-based security to a more proactive, identity-centric framework. This model emphasizes verifying every access request, regardless of origin, to enhance security and operational efficiency.

As work becomes increasingly remote and data more distributed, this approach is crucial for securing sensitive information.

Executive Overview

The Bottom Line

Never trust, always verify.

This means all users, devices, and applications must be authenticated and authorized before accessing resources, regardless of location.

Alignment with Federal Data Strategy

The Zero Trust Model directly supports the broader Federal Data Strategy by:

- Strengthening data protection while maintaining accessibility for authorized users
- Enabling secure data sharing across agencies and departments
- Supporting evidence-based policymaking through secure data access
- Enhancing public service delivery through improved data management

Key Business Impacts

What Changes

- Access to systems and data will require continuous verification
- Security measures will be more granular and automated
- Data handling procedures will become more structured and secure
- System access will be based on specific need rather than general clearance

Key Business Impacts

What Stays the Same

- Core mission operations and services
- Existing data governance frameworks
- Basic workflow processes
- Collaboration capabilities

Implementation Framework

The Five Pillars of Zero Trust

1. Identity Management
2. Device Security
3. Network Security
4. Application Security
5. Data Protection

Implementation Considerations

Resource Requirements

- Initial investment in security technology and tools
- Staff training and development programs
- Potential system upgrades or replacements
- Implementation support and consulting services

Implementation Considerations

Operational Impact

- Minimal disruption to daily operations with proper planning
- Phased implementation to reduce operational risk
- Enhanced security with streamlined access for authorized users
- Improved incident response capabilities

Success Factors

- Active leadership support and engagement
- Clear communication across all organizational levels
- Adequate resource allocation
- Comprehensive change management strategy
- Cross-agency collaboration

Timeline and Key Deadlines

Immediate Actions (Next 30 Days)

- Designate Zero Trust implementation lead
- Begin current security posture assessment

Timeline and Key Deadlines

Short-Term (60-90 Days)

- Submit implementation plan and budget estimates
- Establish data security working group (CDO, CISO)
- Develop initial data categorization framework

Timeline and Key Deadlines

Long-Term (Through FY 2024)

- Achieve specific Zero Trust security goals
- Complete transition to new security framework
- Establish continuous monitoring capabilities

Investment Benefits

- Enhanced protection against cyber threats
- Improved regulatory compliance
- Better control over sensitive data
- Reduced risk of data breaches
- More efficient access management
- Enhanced ability to adapt to future security challenges

Next Steps

1. Review current security practices against Zero Trust requirements
2. Identify critical assets and systems for prioritization
3. Develop comprehensive implementation strategy
4. Begin staff communication and training planning
5. Establish metrics for measuring implementation success

Additional Resources and Support

For detailed technical specifications and implementation guidance, please refer to CISA Zero Trust Maturity Model documentation:

<https://www.cisa.gov/zero-trust-maturity-model>