National Rail Employer Training Seminar - Bureau of Information Services RRB Modernization and Cybersecurity Roadmaps

September 11, 2024

Richard Kramer, Acting Chief Information Officer

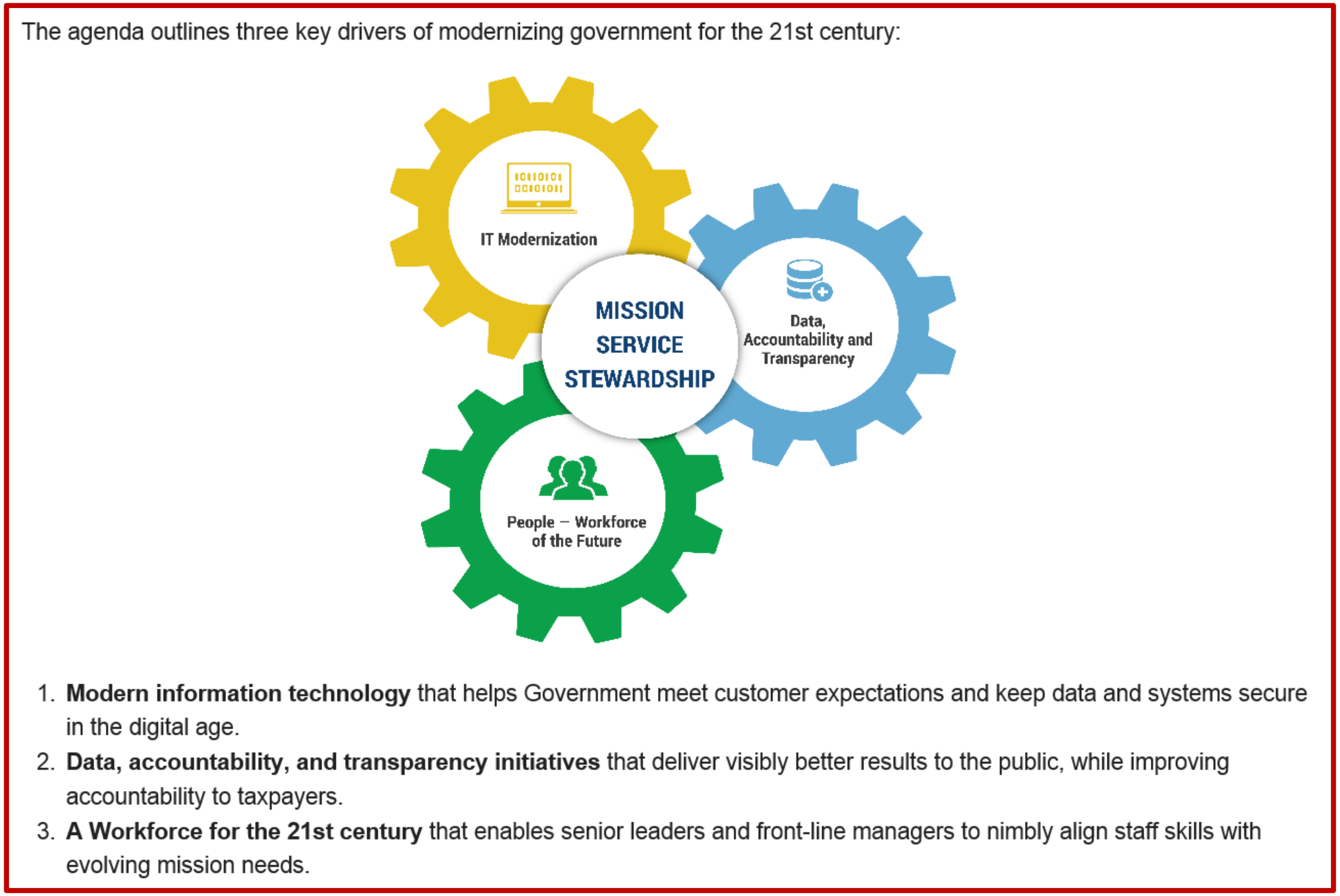
Jerry Gilbert, Chief Information Security Officer

Agenda

- Our Commitment to You
- Modernization
- Cybersecurity
- What It All Means
- Questions?

Our Commitment to You!

- Deliver mission outcomes. Protect customer data. Provide excellent service.



The agenda outlines three key drivers of modernizing government for the 21st century:

IT Modernization
MISSION
SERVICE
STEWARDSHIP
Data, Accountability and Transparency
People – Workforce of the Future

1. **Modern information technology** that helps Government meet customer expectations and keep data and systems secure in the digital age.
2. **Data, accountability, and transparency initiatives** that deliver visibly better results to the public, while improving accountability to taxpayers.
3. **A Workforce for the 21st century** that enables senior leaders and front-line managers to nimbly align staff skills with evolving mission needs.

Our Approach to Modernization

Three-Phases:

Stabilize
Optimize
Perform

- **Stabilize:** *Establish Cloud Presence; Modernize and Secure Infrastructure*
- **Optimize:** *Citizen Experience Improvements; Prepare and Build New, Secure Applications; Secure Data*
- **Perform:** *Transition to Operations & Maintenance*

Throughout these phases:

- **Partner** with Proven Vendors
- Building project and **program management** processes
- **Optimize** along the way

Stabilize Phase Completed Projects:

Migration to Microsoft M365

Physical Mainframe migration to IBM zCloud

- **Streamlines support operations, improving internal efficiency**
- **Reduces technical footprint.**
- **Improves security**

RUIA online Tax forms

- **New services on MyRRB.gov**
- **Reduces Paper and Mailing Cost**
- **Safe, Secure & Convenient**

Completed transition to GSA's EIS contract

- **Improved call-center functionality**
- **Decreased call times to Field Service Offices**

Result: Reduces costs and stabilizes operating environment to allow IT to focus on next modernization phase: *Optimize.*

IRM MODERNIZATION STRATEGIC GOALS

1 - Improve Customer Experience

- 1.1 Data Optimization
- 1.2 Application Modernization
- 1.3 Citizen-Centric Online/Self Service
- 1.4 RRB Customer Improvements

3 – Upskill the IT Team

- 3.1 Identify, Plan, and Implement Technical and Management training
- 3.2 Acquire Contracted Staff to Augment Specialized Skill Sets

2 – Secure the Enterprise

- 2.1 Plan and implement Zero Trust Architecture (ZTA)
- 2.2 Improve Enterprise Security Posture
- 2.3 Establish Sustainable Cybersecurity Operational Support Model

4 – Optimize the Infrastructure

- 4.1 Support ZTA
- 4.2 Migrate Open Systems to Cloud Environments
- 4.3 Optimize Cloud Configuration and Usage
- 4.4 Enhance Privacy and Records Management and Compliance
- 4.5 Improve and Expand Endpoint and Mobility Device Management

What’s Next? Optimize Phase

Use strategies that minimize risk and provide business value.

Modernize our core business functions.

- **Build interfaces to legacy system**
- **Implement application framework**
- **Organize our data**
- **Map business rules**

Result:

- **Methodical approach reduces risk.**
- **Reduce time to deliver system enhancements.**
- **Organized data improves reporting and analytics.**

Our Data Strategy:

Build a "Unified Data Model"

Data will reside in one place.

Architect a comprehensive data analytic solution

Improves picture of mission and operational efficiency.

Promote a culture of continuous data improvement.

New corporate philosophy: Better data helps everyone.

Technology Modernization Fund Initiatives

$1.2B fund for agencies to modernize

9 month process and presentation to a governing board

Not Free – required repayment

- Dec 2022 – RRB receives $8.69M investment for Online Services
- Phase 1 - Change of Address, Direct Deposit – FY2025
- Phase 2 – Sickness Benefit Application
- Internal applications will improve as well; “Customer 360 View”

Key Takeaway:

TMF initiatives build frameworks for future modernization projects which continue to improve our customer’s experience.

Recent Senior Leadership Technology Hires:

Dr. Kathleen McGuire	Chief Data Officer
Dr. Daniel Ostrow	Director, Project Management Office
Cuong “Tony” Nguyen	Associate Chief Information Officer, Infrastructure Services
M. Faheem Naushad	Associate Chief Information Officer, Enterprise Applications.

Cybersecurity. In the News!

How is the RRB preparing for the increased threats?

- Top 2024 attacks(Ivanti Connect Secure VPN attack including attacks on CISA and Mitre, Microsoft Executive Accounts Breach, SOHO router attacks by China, AT&T breach)
- Increased attacks from nation state (i.e. China, Russia, North Korea.)
- M-24-14, Administration Cybersecurity Priorities for the FY 2026 Budget
- Implementing Zero Trust (ZTA).
- The RRB integrate security requirements from the beginning of every project and through the entire system development lifecyle (SDLC).

Implementing Zero Trust Security

A Modern Approach to Cybersecurity
Jerry Gilbert (CISO)

<u>Introduction to Zero Trust</u>

- Definition: Zero Trust is a security model that assumes threats could be internal or external.

- **Key Principle: "Never trust, always verify.“**

<u>Why Zero Trust?</u>

- Increase in Cyber Threats: Statistics on breaches.

- Traditional Perimeter Security Limitations: Issues with VPNs and firewalls.

- Shift to Remote Work: Rise in cloud services and remote access.

Zero Trust Maturity Journey

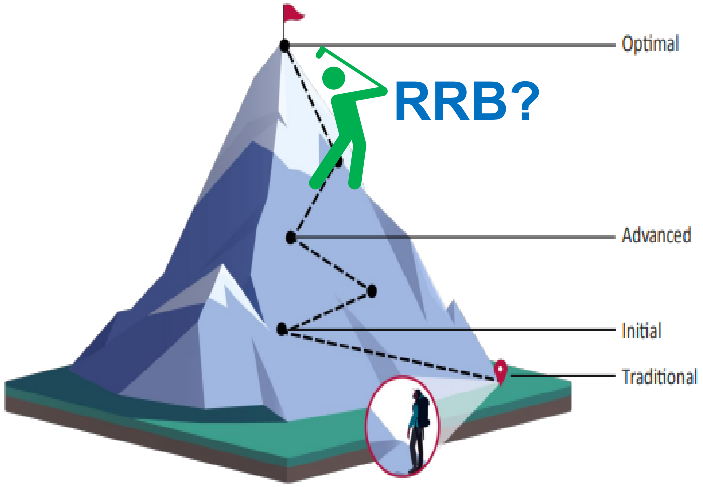


Figure 2: Zero Trust Maturity Journey

Zero Trust Working Group? A better way?

Q? How about a single working group that <u>brings together </u>the disciplines?
(Service, Security, Compliance, GRC/RMF, Privacy, Data, Records Management etc.).

Jerry's input: these priorities

1. Identity
2. Device
3. Apps

Integrated

Formulate strategy for

- Data for 2025
- Apps for 2025

ZT activities in parallel:

- OMB M-22-09
- Network segmentation
- User training
- App rationalization
- SecOps Advanced Hun
- SecOps Playbooks
- M365 Insider Risk

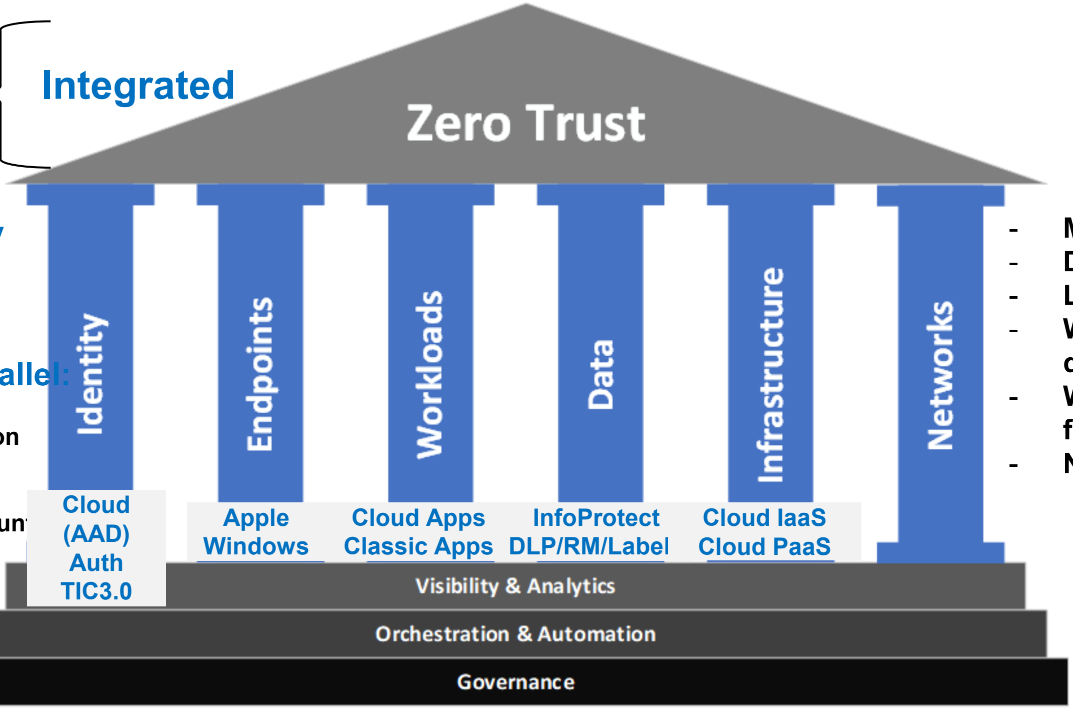


Figure: The Zero Trust Maturity Model with added Infrastructure Pillar.

- Maturity outcomes
- Don't forget the foundations
- Leads for each Pillar?
- We can meet monthly or quarterly.
- We can guide IT projects in flight.
- Not just security.

ZTA

Core Principles of Zero Trust
- Verify identity and device at every access attempt.
- Limit access to the minimum necessary.
- Assume a breach: Respond proactively.

Key Components of Zero Trust
- Identity and Access Management (IAM)
- Multi-Factor Authentication (MFA)
- Network Segmentation
- Encryption
- Continuous Monitoring and Analytics

Benefits of Implementing Zero Trust
- Enhanced Security Posture
- Reduced Attack Surface
- Improved Compliance
- Greater Visibility into Network Activity

Overview: Microsoft's Zero Trust Principles

Core principles, but much more.
Keep these fundamentals in mind.
Simplify the message for the business.
Simplify the message for the users.

For CISOs: Inform the Users (3 simple things)

1. Protect your identities
2. Protect your devices
3. Protect your data

1. Verify explicitly

Always validate all available data points (AAD Conditional Access)

- Users (identity, location, risk score)
- **Groups & service principals**
- Devices (**identity,** health, risk score)
- **Apps & browsers**
- **Data, asset sensitivity**
- Service or workload context
- Other anomalies

2. Use least-privilege access

Limit and threat-manage user and Admin access (see below)

- **Role Based Access Control (RBAC)**
- **Just-in-time access (JIT)**
- **Just-enough-access (JEA)**
- **Risk-based adaptive policies**
- **Data protection against out of band vectors**
- **Deep monitoring > insider risk**

3. Assume breach

Minimize blast radius for breaches and prevent lateral movement:

- **Harden systems as if they're publicly accessible, encrypt everywhere.**
- **Segment access by network, user, devices, apps.**
- **Integrate Cyber and Monitoring: SIEM/SOAR/CASB/EDR - integrated**
- **AI+analytics for threat detection, posture visibility and improving defenses.**

ZTA

Steps to Implement Zero Trust

1. **Assess Current Security Posture**
   - Evaluate existing infrastructure and policies.
2. **Define the Protect Surface**
   - Identify critical data, assets, applications, and services (DAAS).
3. **Map the Transaction Flows**
   - Understand how users access resources.
4. **Implement Identity and Access Management**
   - Adopt strong authentication methods.
5. **Micro-Segmentation**
   - Limit lateral movement within the network.
6. **Monitor and Maintain**
   - Use continuous monitoring tools for real-time insights.

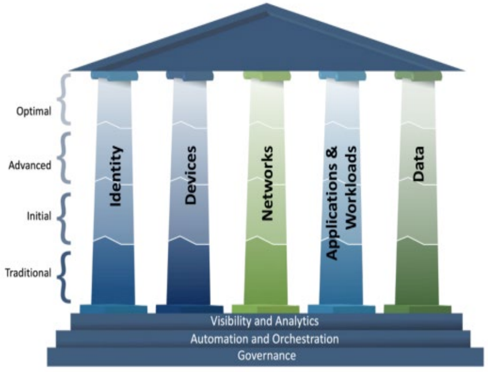
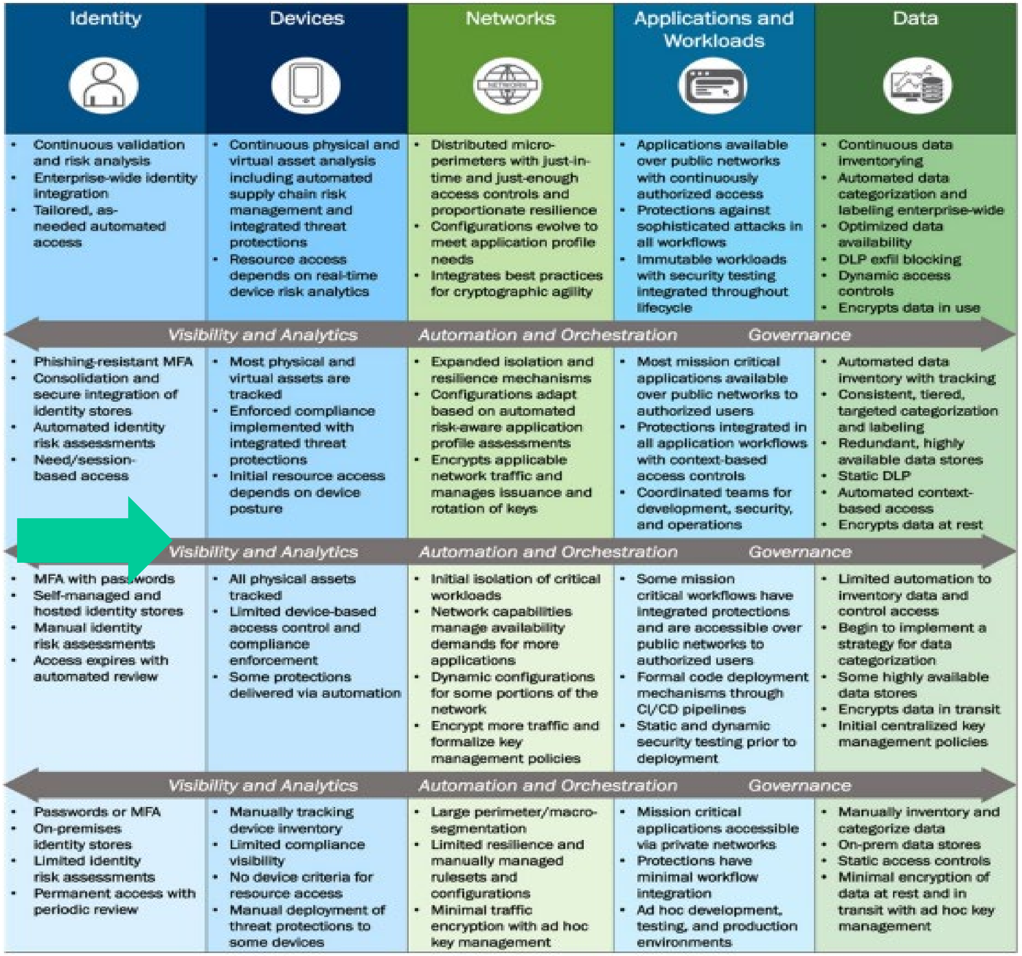


Figure 3: Zero Trust Maturity Evolution



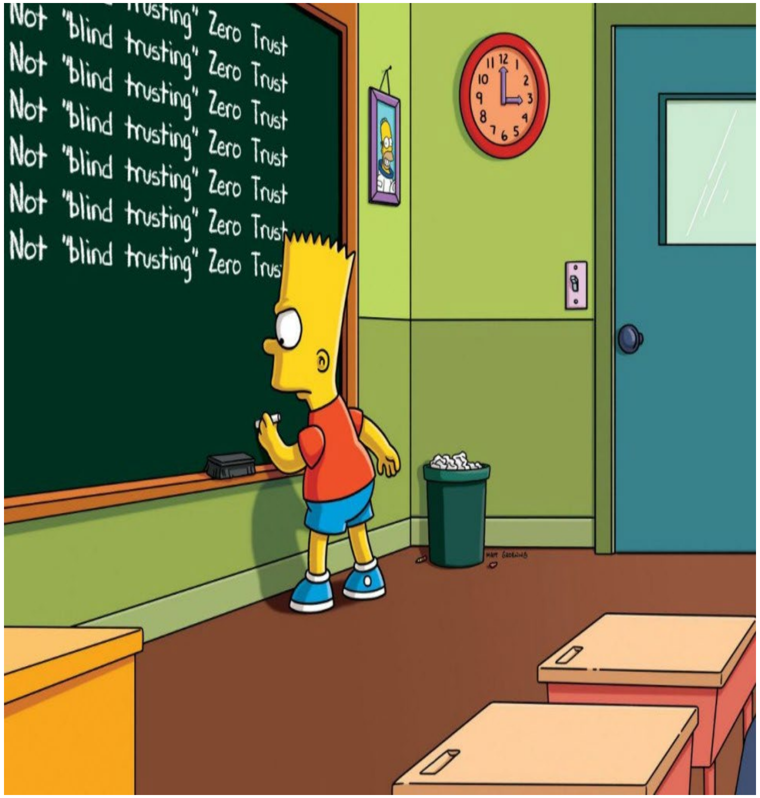
	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
	Visibility and Analytics		Automation and Orchestration	Governance	
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
	Visibility and Analytics		Automation and Orchestration	Governance	
Initial	• MFA with passwords • Self-managed and hosted identity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorization • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
	Visibility and Analytics		Automation and Orchestration	Governance	
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

Figure 4: High-Level Zero Trust Maturity Model Overview

ZTA

<u>Challenges in Implementation</u>

- Complexity of Integration
- User Resistance
- Cost Considerations
- Need for Continuous Education and Training


Not "blind trusting" Zero Trust
Not "blind trusting" Zero Trust
Not "blind trusting" Zero Trust
Not "blind trusting" Zero Trust
Not "blind trusting" Zero Trust
Not "blind trusting" Zero Trust
Not "blind trusting" Zero Trust

What It All Means:

- Improve and enhance available online services.
- Implement technologies that continue to reduce paper processing.
- Receive information from multiple citizens (annuitants, medical professionals, and railroads) electronically and securely.
- Improve security.
- What other items should we focus on?

Q & A