National Reporting Officers Meeting - Bureau of Information Services RRB Modernization and Cybersecurity Roadmaps

August 5, 2021

Richard Kramer, Deputy Chief Information Officer
Jerry Gilbert, Chief Information Security Officer

Agenda

- Our Commitment to You
- A Quick Look at the Past
- 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:

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.

A quick look at the last 18 months…..

- Pandemic required near 100% work-at-home status while still providing the same level of customer service to the rail community.
- Several initiatives were quickly implemented:
  - New Internet connection was implemented to better support 700+ RRB staff working remotely.
  - Cell phones were provided to all staff to aid communications and expand services.
  - Creative solutions were found to convert legacy “paper” systems into digital ones.
- The pandemic forced us into a new operational support model which taught us lessons that will be incorporated into future modernization efforts.

Completed Projects since 2018:

RRB.GOV moved to Amazon Web Services	• Multi-regional disaster recovery and resiliency • Enhanced security
Improvements to ERSNet	• Modernized code processing • Increased system performance
Use of Pay.gov to submit contribution payments	• Safe, Secure & Convenient • Reduces Paper and Mailing Cost • It's a FREE Service to Employers

Result: Reduces risks and improve services for you.

Our Approach to Modernization

Three-Phases:

- **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:

- **Reskill/Upskill** Existing Team
- **Partner** with Proven Vendors
- Building project and **program management** processes
- **Optimize** along the way

Current phase: Stabilize

- Working with other RRB business units to identify opportunities to improve services for both internal and external citizens.
- Implementing a Program Management Office to manage the modernization effort and funding.
- Partnering with industry leaders to aid in our modernization efforts.
- Investigating contracting opportunities to obtain additional services and skillsets.
- Targeted investments in technology that address greatest risks to stability and security.
- Continuing to perform discovery and gathering requirements for modernization phase.

Current Stabilize Projects

Migration to Microsoft M365

Physical Mainframe migration to IBM zCloud

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

Result:

Stabilizes operating environment to allow IT to focus on next modernization phase: *Optimize.*

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**

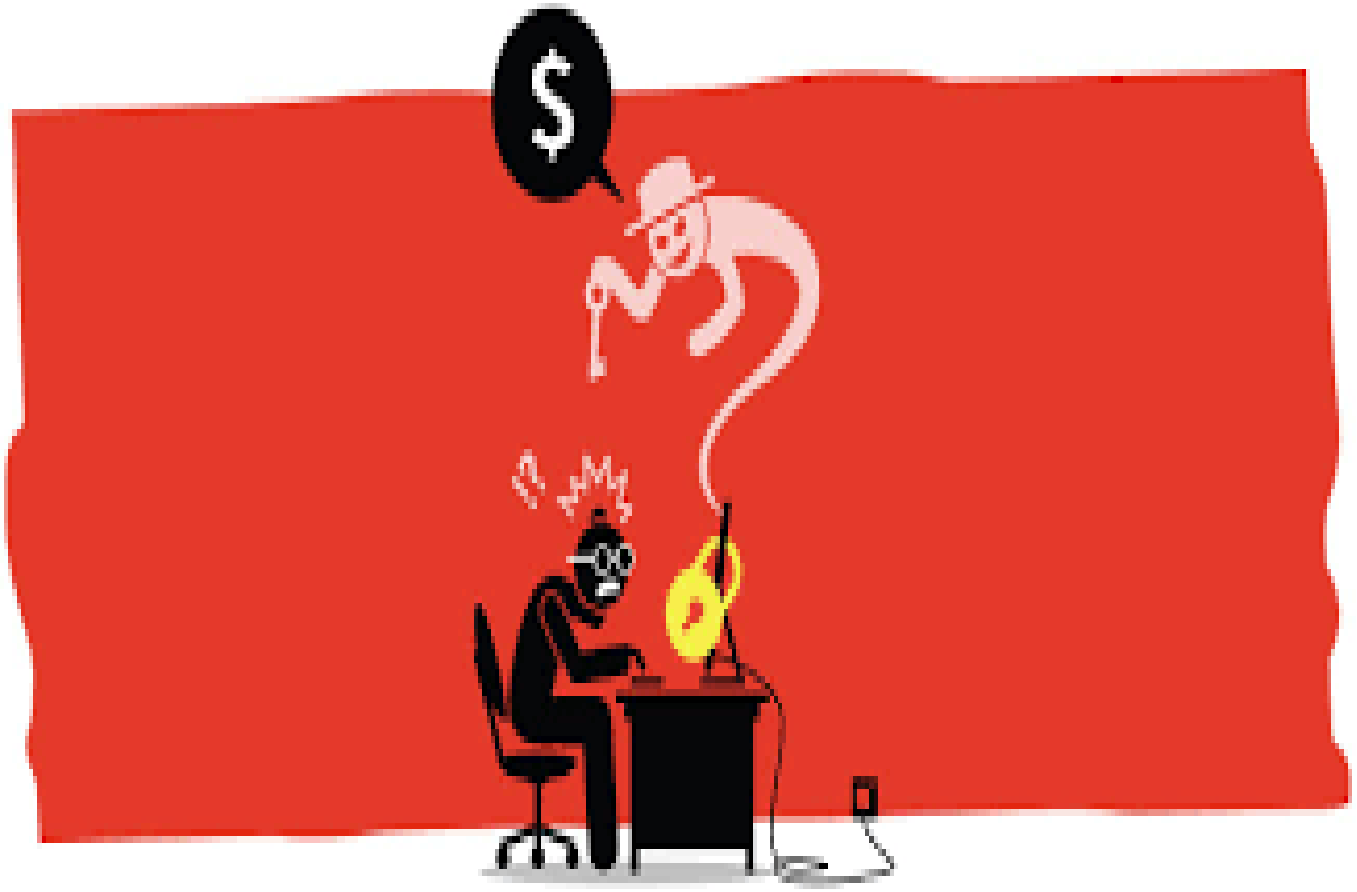
Result:

- **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.**

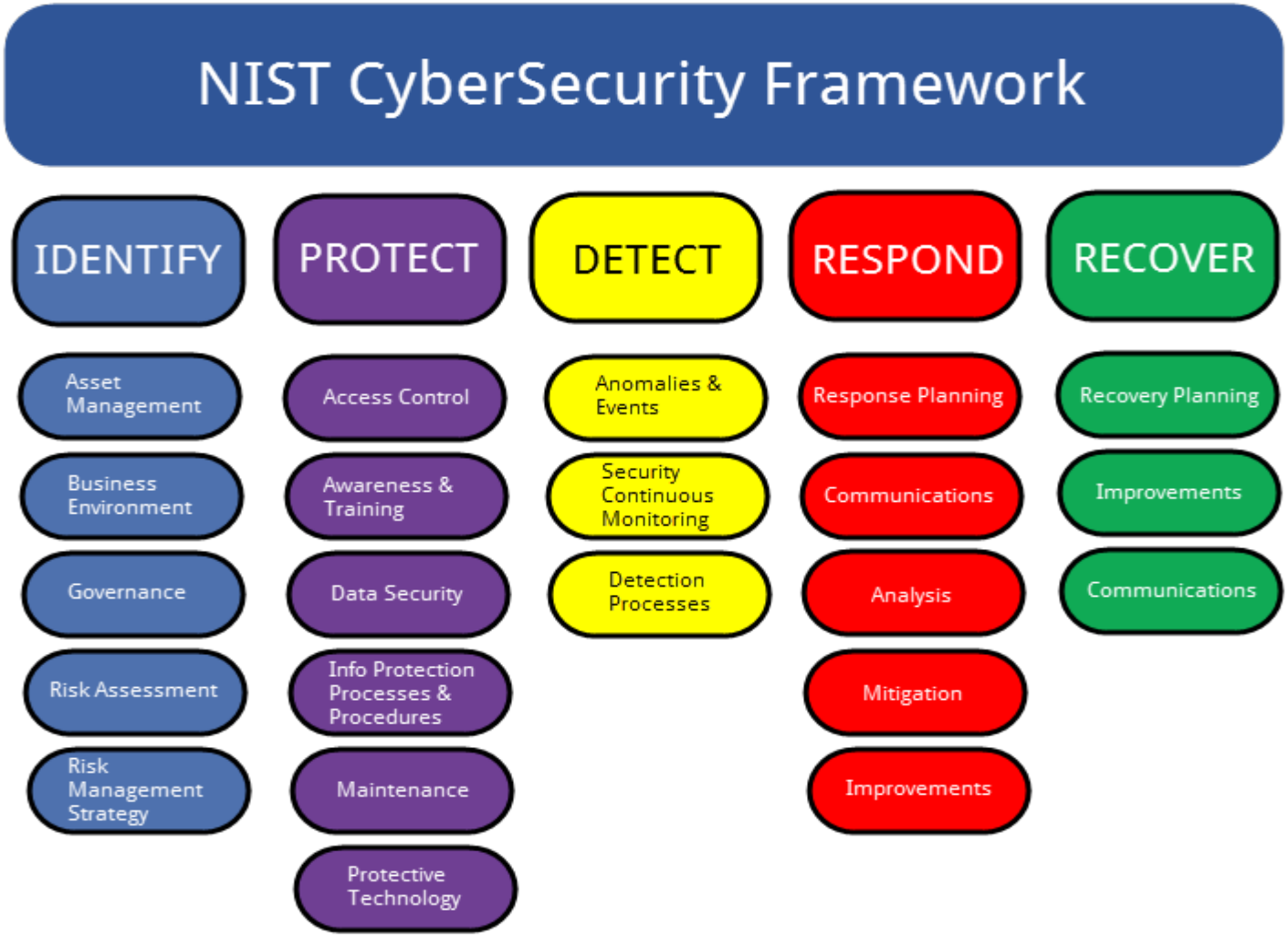
Cybersecurity. In the News!



How is the RRB preparing for the increased threats?

- Ransomware risk (the Colonial Pipeline, Steamship Authority of Massachusetts, JBS (world's largest meatpacker, and the Washington DC Metro Police.)
- Increased attacks from nation state (i.e. China, Russia, North Korea.)
- Supply Chain threats (i.e. Solarwinds attack in December)
- Executive Order on Improving the Nation's Cybersecurity in May 2021
- The Cybersecurity Framework helps to improve the cyber resilience against threats.
- We integrate security requirements from the beginning of every project.

The Cybersecurity Framework helps to improve the RRB cyber resilience against threats.



Identify - Foundational for effective use of the Cybersecurity Framework.

- DHS Continuous Diagnostic and Mitigation(CDM) program
  - CDM Hardware Asset Management (HWAM)
  - CDM Software Asset Management (SWAM)
  - CDM Configuration Management
  - CDM Vulnerability Assessment
- CDM Federal Dashboard
  - AWARE score
- Updated RRB Information Security Policy to NIST SP 800-53 revision 5, Security and Privacy Controls for Information Systems and Organizations

Protect – Developing and implementing the appropriate safeguards.

- Access Control - Trusted Internet Connection (TIC 3.0)
  - Cloud and public access
- Awareness and Training
  - Phishing awareness
- Data Security
  - Data Loss Prevention (DLP)
- Identity, Credential, and Access Management (ICAM)

Detect – Developing and implementing the appropriate activities to identify the occurrence of a cybersecurity event.

- Microsoft (MS) Defender
  - MDI – MS Defender for Identities
  - MDE – MS Defender for Endpoint
  - MDAV – MS Defender Antivirus
- Microsoft Sentinel
  - SIEM – Security Information and Event Manager
- Cisco Intrusion Prevention/Intrusion Detection (IPS/IDS)

Respond – Developing and implementing the appropriate activities to take action regarding a detected cybersecurity event.

- **RRB's Security Operation Center (SOC) staff are fully capable of responding to all cybersecurity events.**
- **Cybersecurity tools described in Detect category enhance the SOC teams ability to respond to cybersecurity events**
- **SOC staff attend leading edge training annually (i.e. SANs) to ensure they are abreast of all the latest developments in the information security field.**

Recover – Developing and implementing the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

- Aligns with CIO's modernization strategy.
- Microsoft Azure and M365
- IBM z-Cloud.

What It All Means:

- Improve and enhance available online services.
- Implement technologies that continue to reduce paper processing.
- Receive medical information from multiple citizens (annuitants, medical professionals, and railroads) electronically and securely.
- Expand the use of secure, encrypted email for our citizens.
- Align workloads with the correct RRB functional groups.
- Improve security.
- <u>What other items should we focus on?</u>

Q & A