Citizen Oversight Panel Briefing

Information Technology Update

Presenters:
Jason Weiss, CIO
Alex Di Giacomo, CISO

July 21, 2021

SOUNDTRANSIT

Agenda

1. Technology Strategy – *Jason Weiss, CIO*
2. Information Security Overview – *Alex Di Giacomo, CISO*

IT Overview

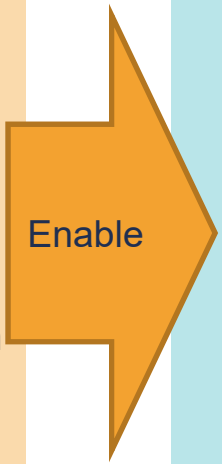
Strategic Priorities (Aligned to Agency 5 Year Strategic Plan)

1. Clear and Effective IT Engagement
2. Effective and Consistent IT Delivery
3. IT Service Availability
4. Data Driven Transformation
5. Digital Workforce Enablement

IT Overview - Technology Strategy

Technology Strategy

1. Clear and Effective IT Engagement
2. Effective and Consistent IT Delivery
3. IT Service Availability
4. Data Driven Transformation
5. Digital Workforce Enablement



5 Year Agency Strategic Plan

1) Design and deliver a passenger-focused, high-quality and safe service
2) Deploy a performance-based, community-centric and safe capital program
3) Cultivate an equitable, diverse and inclusive workforce and culture that is high-performing, compassionate, empowering and safe
4) Transform and unify core business practices and processes agencywide
5) Ensure financial stewardship exists in all decision-making to guarantee long-term affordability of the voter-approved plan

IT Overview - Technology Strategy

1. **Clear and Effective IT Engagement**
   - Why? Agency evolving; ST's services in Operations growing as the voter approved expansion plan advances
   - IT as a strategic partner aligned to business goals
   - Major technology investments aligned to Agency Strategic Plan

Major, Active Programs:

- Next Gen ORCA
- Passenger Information Program – improved and expanded passenger information: mobile, web, digital signs

IT Overview – Technology Strategy

2. **Effective and Consistent IT Delivery**
   - Why? Larger agency (and IT Dept) following years of rapid growth necessitates change to effectively handle increased workload
   - Scaling core IT process; end-to-end delivery of IT services to the agency
   - Building IT services that are: business aligned, consistent, efficient, secure

IT Overview – Technology Strategy

3. IT Service Availability

- Why? Ensure core systems uptime & resiliency in a growing system, with growing complexity and risk
- Transit/control systems as expansion continues
- Passenger facing systems
- Administrative systems – core business functions of the agency

Major, Active Programs:

- Agency Network Program – rebuilding core networks for ST3
- Information Security Program – more information ahead….

IT Overview – Technology Strategy

4. Data Driven Transformation

- Why? Enabling agency strategic plan priorities, including Strategic Asset Management ISO compliance goal
- Improve data quality & consistency, including internal as well as public & rider data
- Improve decisions informed by data

Major Programs:

- Agency Data Management Program – proposed 2022 priority

IT Overview – Technology Strategy

5. Digital Workforce Enablement

- Why? enable increased flexibility, enhanced communications, and improved productivity for staff agency-wide
- Drive agencywide adoption of modern technology platforms
- COVID era remote work led to rapid gains
- Evolving to Hybrid, while maintaining the gains of past year

Major Active Projects:

- Office365 Migration (Trailblaze)
- Hybrid enablement

Information Security Overview

Data Classification: Unrestricted

Why we are here…

- To provide background and context on the relevance of Information Security issues to the agency, and an overview of the agency's efforts to address relevant risks

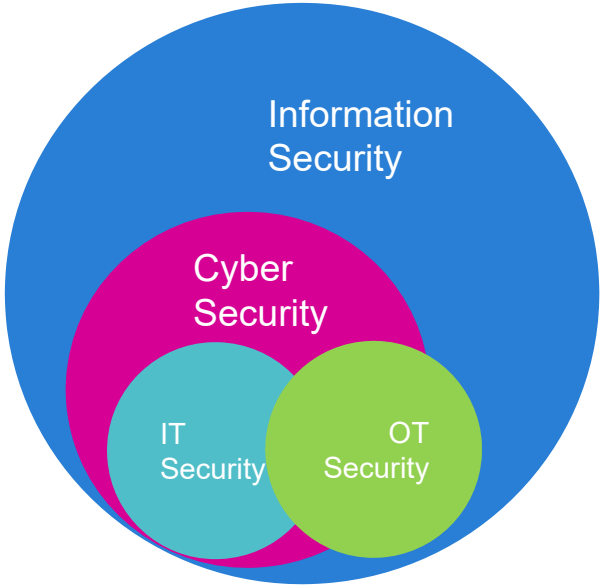
- To answer any questions from the Panel

Background – ST leads, Transit Industry Lags

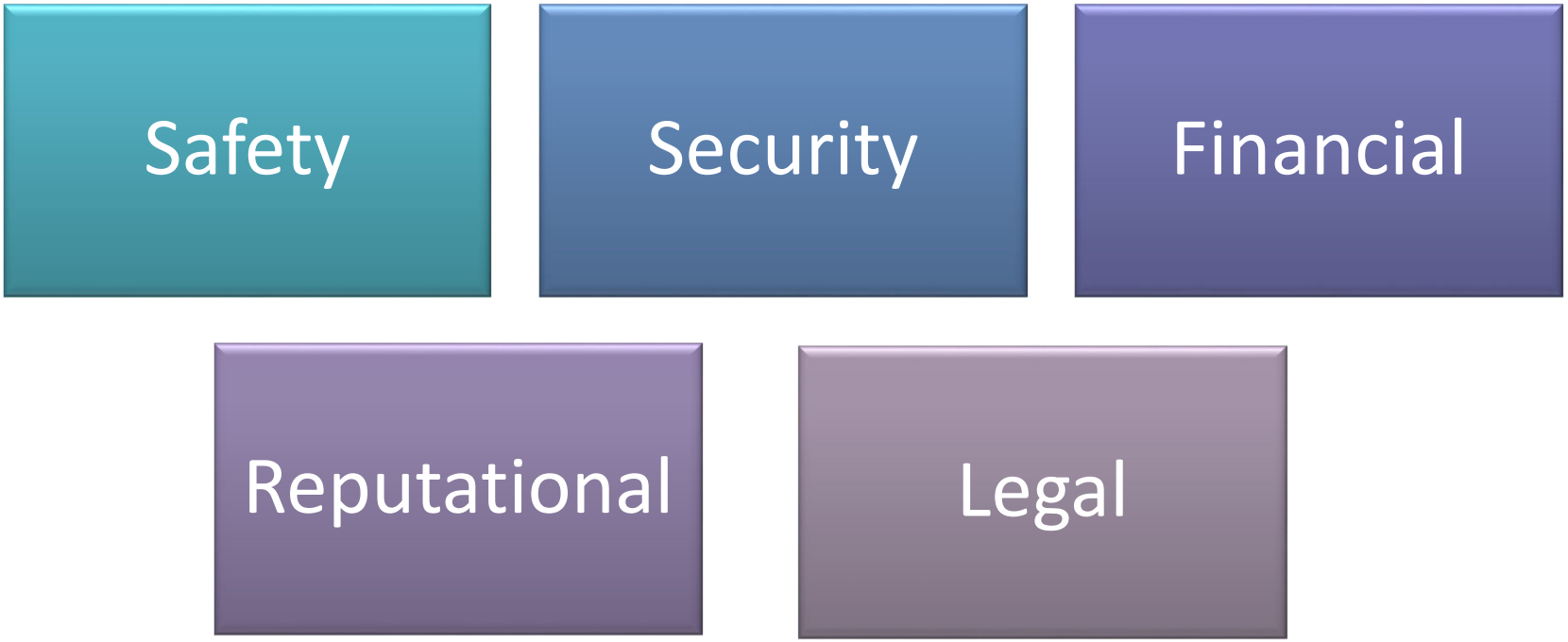
- Sound Transit is one of few transit agencies in the country who have formally recognized the need for a dedicated Information Security function – Peers include New York MTA, BART, DART, WMATA and MARTA
- Federal regulations are expected to prompt significant changes in the security of critical infrastructure cyber assets, in line with current regulations applicable to the Energy sector
- Sound Transit's Information Security program is five years old and is led by the Chief Information Security Officer, and overseen by an Information Security Risk Council comprised of the Deputy CEOs, the CIO and the CISO
- The Information Security program is administered by the Information Security Division of IT, has agency-wide coverage, and is based on the ISO 27001:2017 international standard for Information Security
- Prior to the program launch, ownership of Information Security practices and control was distributed amongst functional teams, with no centralized subject matter oversight – Systems were not explicitly designed for security (common previous practice in Transit)

Information Security: Broader than IT Security

Information Security: Broader than IT Security



Information Security Impacts Many Areas



Relevant News

Photographer: Samuel Corum/Bloomberg

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

By William Turton and Kartikay Mehrotra
June 4, 2021, 12:58 PM PDT

- Investigators suspect hackers got password from dark web leak
- Colonial CEO hopes U.S. goes after criminal hackers abroad

POLITICS

Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate

PUBLISHED TUE, JUN 8 2021•10:17 AM EDT | UPDATED WED, JUN 9 2021•8:24 AM EDT

Christina Wilkie
@CHRISTINAWILKIE

SHARE

Colonial Pipeline Cyberattack Proves a Single Password Isn't Enough

Since the attack, it's been revealed that it was down to a single password. Yes, ransomware needs to be on your radar -- but a focus on credentials is vital.

Dark Reading Staff
Dark Reading

June 14, 2021

Relevant News

AP

Fallout continues from biggest global ransomware attack

By FRANK BAJAK July 5, 2021

BUSINESS

Russian cyber gang REvil, blamed for global ransomware attack, disappears

By Will Feuer July 14, 2021 | 9:35am | Updated

ZDNet

Ransomware: We need a new strategy to tackle 'exponential' growth, says Interpol

Important Considerations for Transit and other Government Agencies

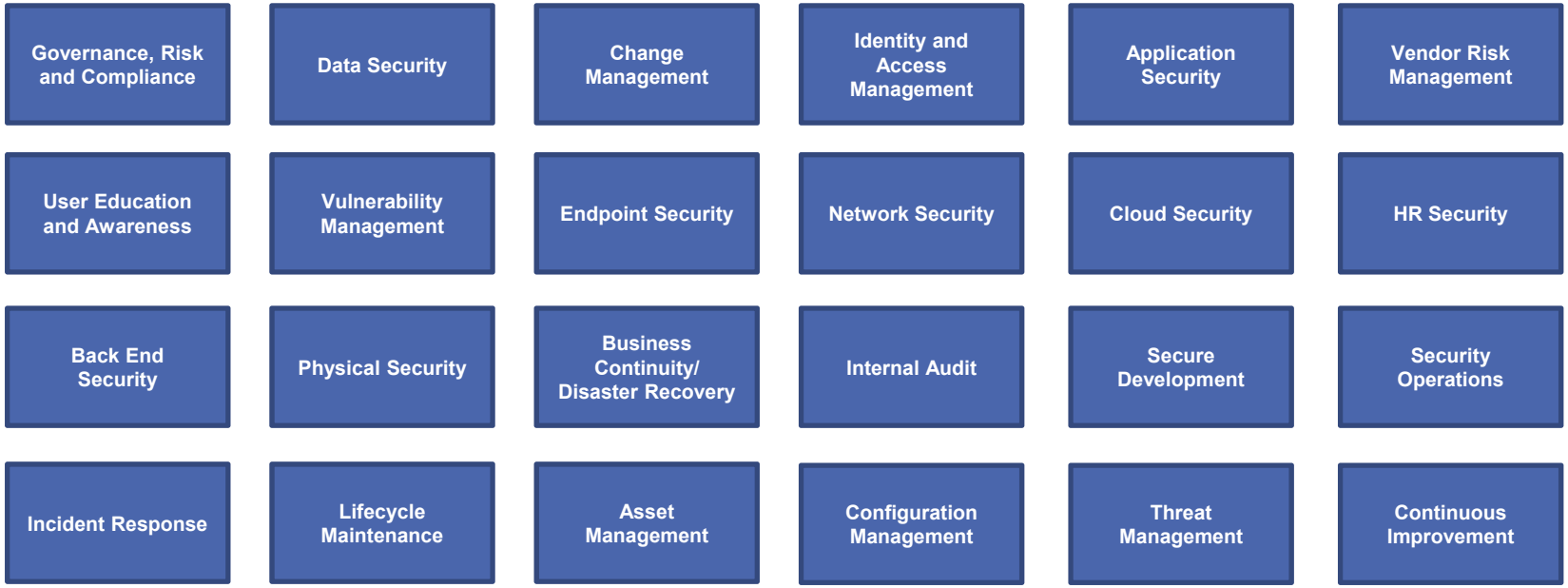
- Government is actively being targeted
- Federal Regulation is looming – DHS CISA
- Attacks consistently exploit the fundamentals
- Financial losses resulting from attacks are increasing

A Formalized Organizational Function is needed, with Programmatic Approach

Vision: To develop and maintain an organizational function that allows the Agency to systematically identify, evaluate, and address risks to the security of the information and technology resources that it requires to fulfill its mission

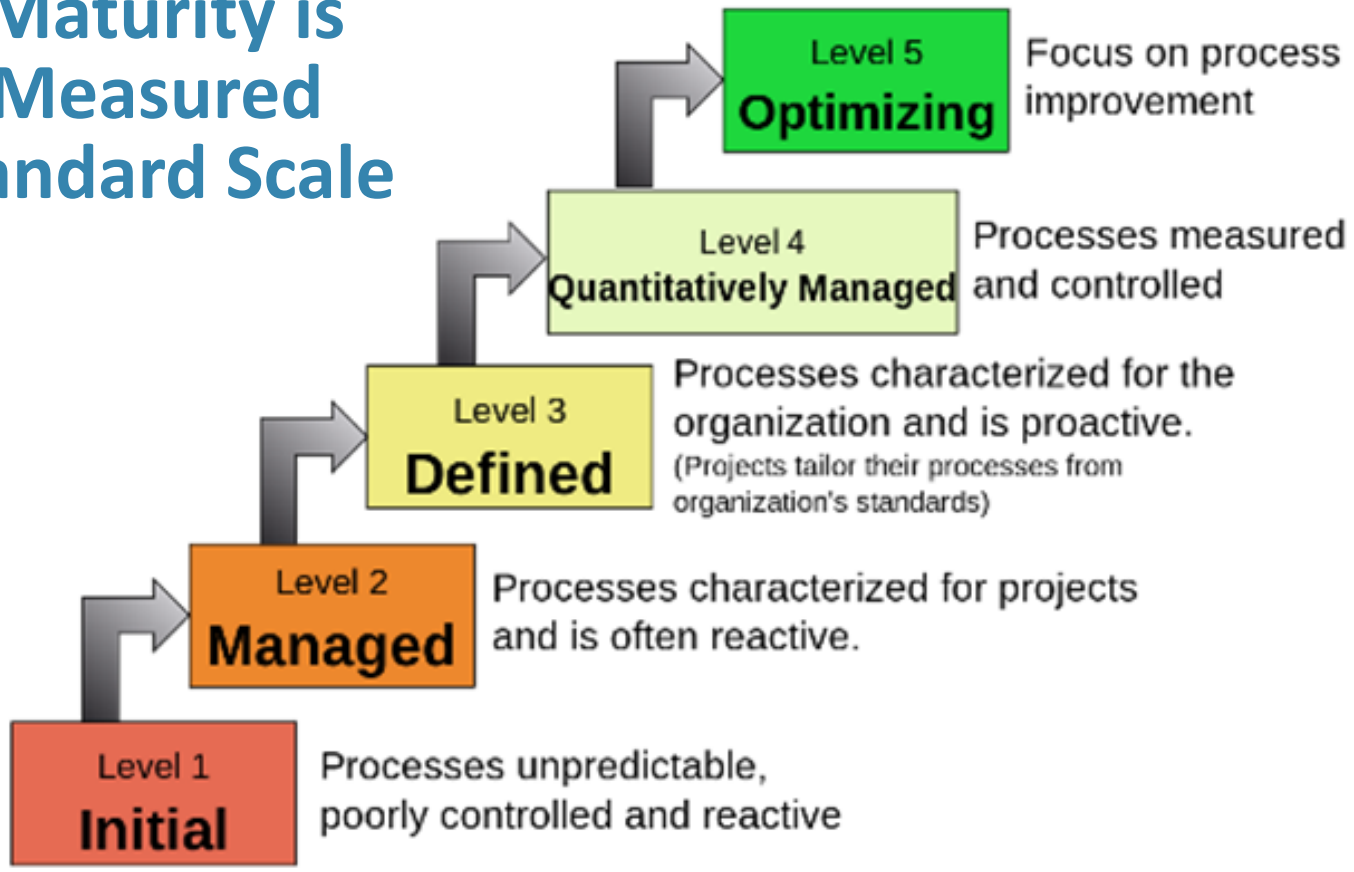
An Effective Program Encompasses Elements from Several Dimensions

An Effective Program also Encompasses Elements from many Functions and Areas

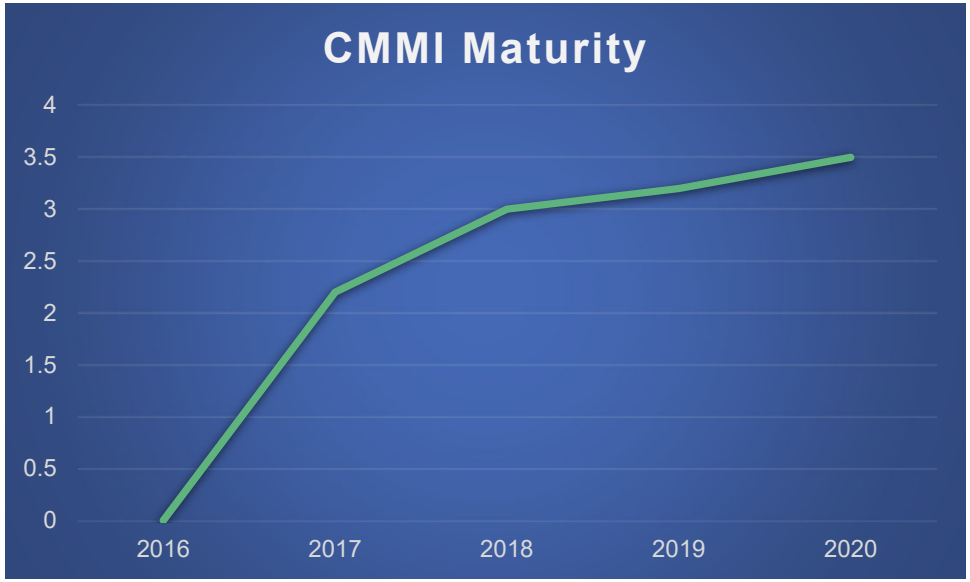


InfoSec Program – Main Objectives

Program Maturity is Typically Measured with a Standard Scale



Where we are – Maturity

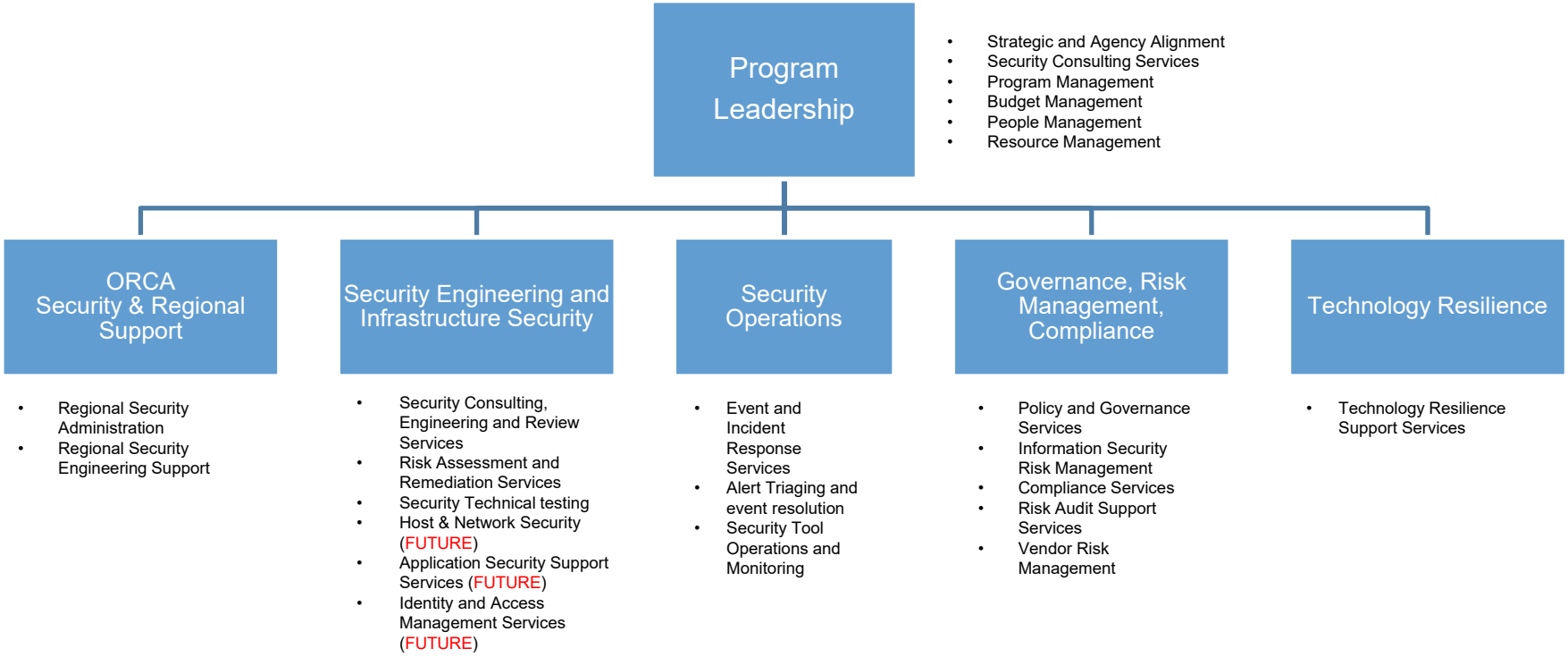


Where we are - Objectives

An Effective Program also Encompasses Elements from many Functions and Areas

An Effective Program also Encompasses Elements from many Functions and Areas

InfoSec Division Functional Organization



There are Tangible Opportunities for Improvement through the Program

- Prioritize investments in InfoSec function
- Adopt enterprise approach to control Information Security risks across all agency functions
- Transform our culture so it reflects the importance of InfoSec objectives
- Focus on remediation of identified, existing technical and process issues

Key Focus Areas for Program Success

Next Steps for the InfoSec Program

- Ensure Information Security objectives are explicitly included into agency strategy
- Focus on controlling current risks, particularly in the Operations Technology (OT) space
- Continue to embed the services of the Information Security Division into all agency functions
- Build all new systems, including capital expansion projects, with Information Security controls from the ground up

Discussion - Q&A

Thank you.

SOUNDTRANSIT

soundtransit.org

Data Classification: Unrestricted