The National Academies of
SCIENCES · ENGINEERING · MEDICINE

TRANSPORTATION RESEARCH BOARD

Strategically Implementing Transportation Security Measures

April 28, 2021

@NASEMTRB
#TRBwebinar

PDH Certification Information:

- 1.5 Professional Development Hour (PDH) – see follow-up email for instructions
- You must attend the entire webinar to be eligible to receive PDH credits
- Questions? Contact Reggie Gillum at RGillum@nas.edu

The Transportation Research Board has met the standards and requirements of the Registered Continuing Education Providers Program. Credit earned on completion of this program will be reported to RCEP. A certificate of completion will be issued to participants that have registered and attended the entire session. As such, it does not include content that may be deemed or construed to be an approval or endorsement by RCEP.

RCEP

REGISTERED CONTINUING EDUCATION PROGRAM

#TRBwebinar

Learning Objectives

1. Identify challenges and opportunities related to security practices at state DOTs
2. Leverage existing tools and resources to enhance current security parameters
3. Integrate and assess change management elements when implementing security practices at the enterprise, program, project, and activity levels

Strategically Implementing Transportation Security Measures

April 28, 2021

Research Team

Chelsea Treboniak
Critical Ops, LLC

Michael Audino
University of South Florida (USF) – Center for Urban Transportation Research (CUTR)

Debbra Johnson
Debbra A.K. Johnson, LLC

Jennifer Hesterman
Security Expert

Ally Pinheiro
Critical Ops, LLC

Silvana Croope
University of Alabama – Alabama Transportation Institute (ATI)

Doug Clifford

Gary Ackerman

University of Albany State University of New York College of Emergency Preparedness, Homeland Security, Cybersecurity

Contributors

Stephen Terhaar
Facility Operations and Security Director
Minnesota Department of Transportation

Neal Murphy
Emergency Management Planner
Idaho Transportation Department

Is security important to you?

Is security important to your organization?

Why are you here?

Learn how to incorporate security practices into daily activities – become a force multiplier.

Share thoughts and concerns on security in the workplace and receive feedback from experts in the field.

Become part of a community influencing changes to security thinking in transportation.

Make the lives of the people that we serve better.

Agenda

- Research Overview
- Minnesota Department of Transportation Case Study
- Idaho Transportation Department Case Study
- Bridges Case Study
- Cybersecurity Case Study
- Security Implementation Tool and Benchmarks
- Q&A

Project Objectives

Develop and support implementation of a strategy for transportation security in state Departments of Transportation (DOTs).

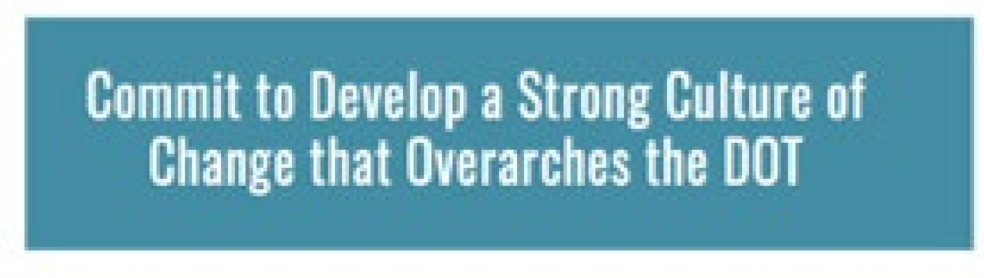
Facility-based security, infrastructure-based security, and event-based security.

Increase security practices at state DOTs.

Project Plan

Phase I: Jan – Dec 2020

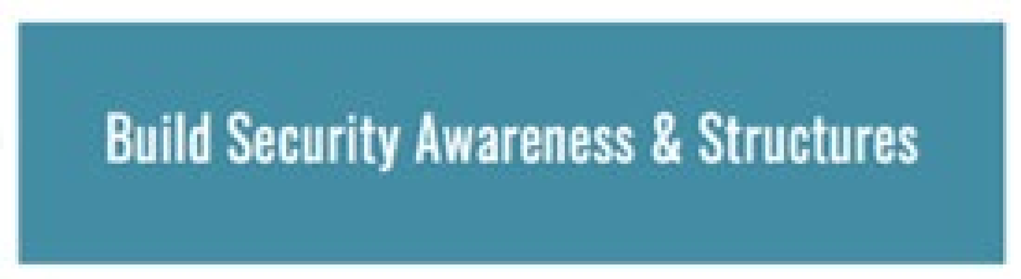
- Tasks 1-4
- Academic Foundation
- Practitioner Insights
- Gap Analysis
- Security Guidelines Deployment Strategy



Commit to Develop a Strong Culture of Change that Overarches the DOT

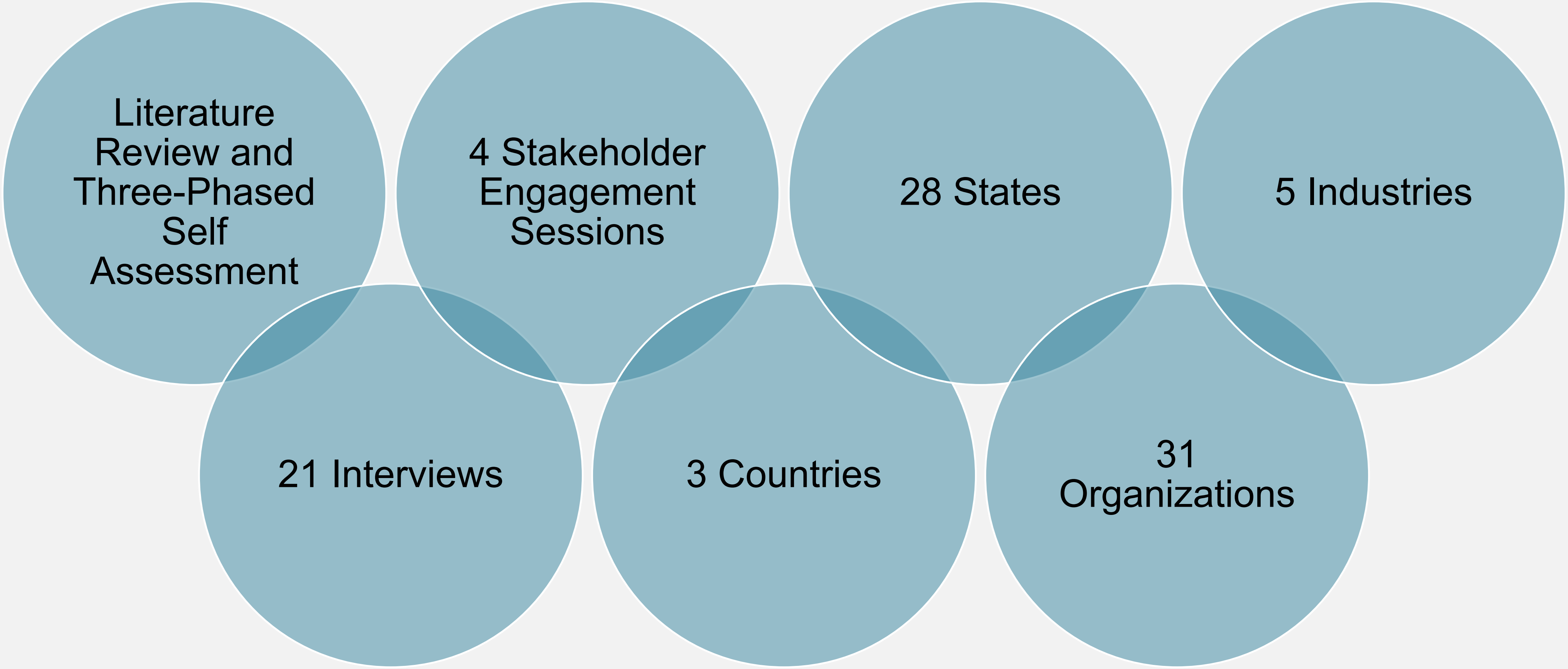
Phase II: Jan 2021 – Jul 2022

- Tasks 5-8
- Security Training and Educational Toolkits
- Pilot Tests
- Implementation



Build Security Awareness & Structures

Data Collection



Literature Review and Three-Phased Self Assessment

4 Stakeholder Engagement Sessions

28 States

5 Industries

21 Interviews

3 Countries

31 Organizations

Insights

- Security Awareness
- Customized Integration – Processes, Planning, Programs, and Budgets
- Enforceable Security Standard – Accountability
- Operational Separation

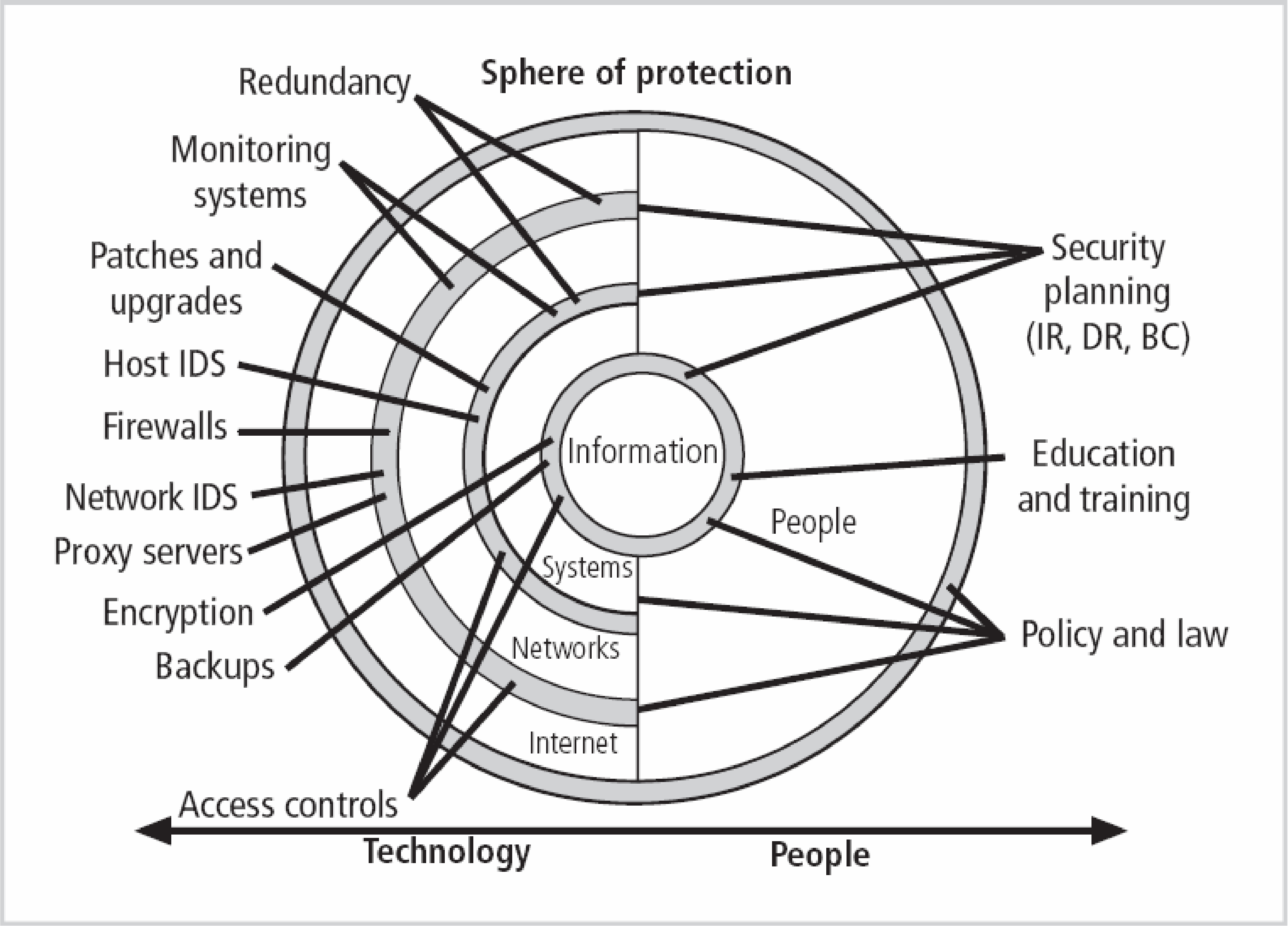


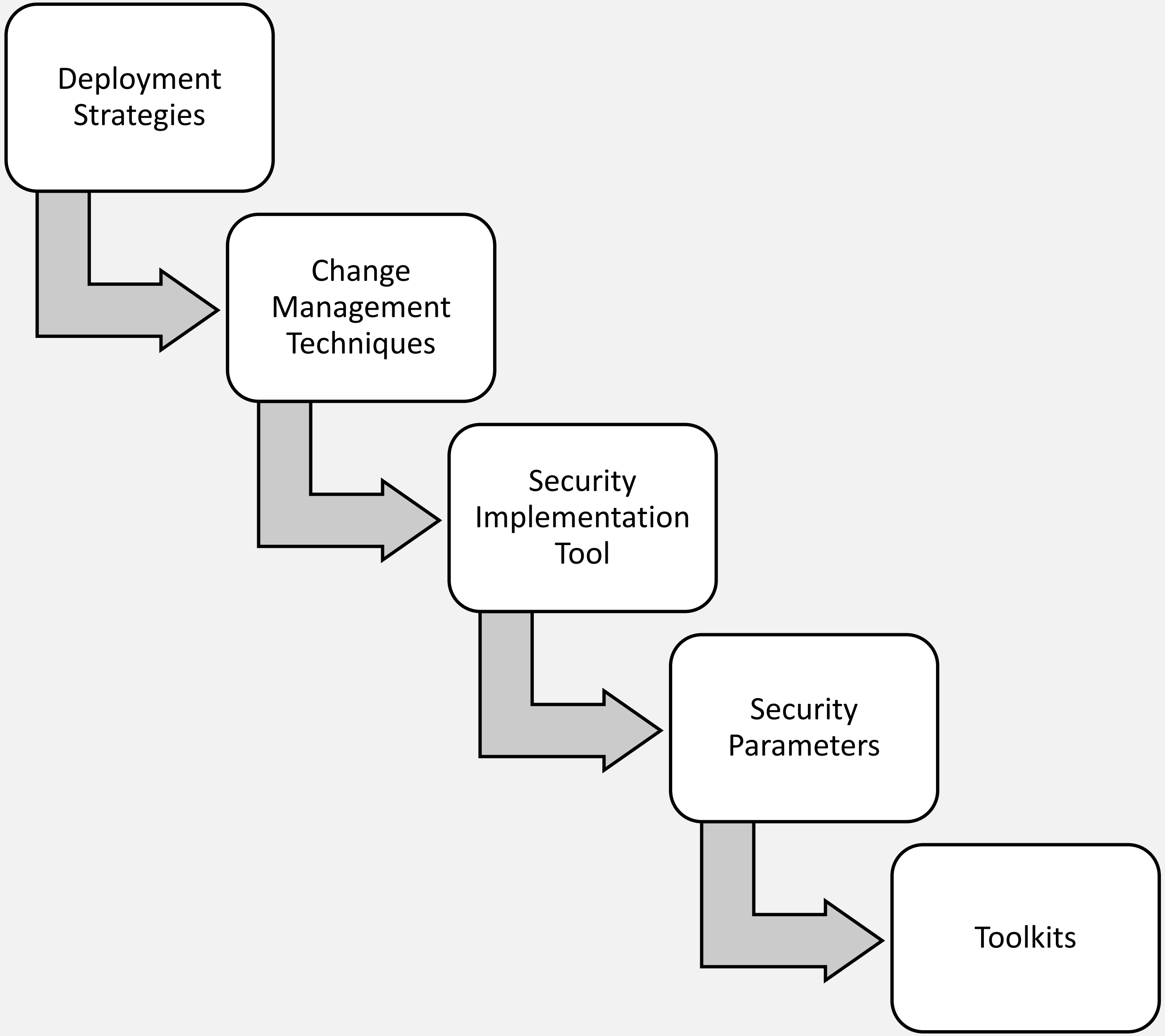
FIGURE 9-1 Sphere of Security

Source: Management of Information Security, 2nd ed. - Chapter 9

Infrastructure:

- Fundamental Facilities and Systems
- Support the Sustainable Functionality

Actions & Outputs – Security Guidelines Deployment Strategy



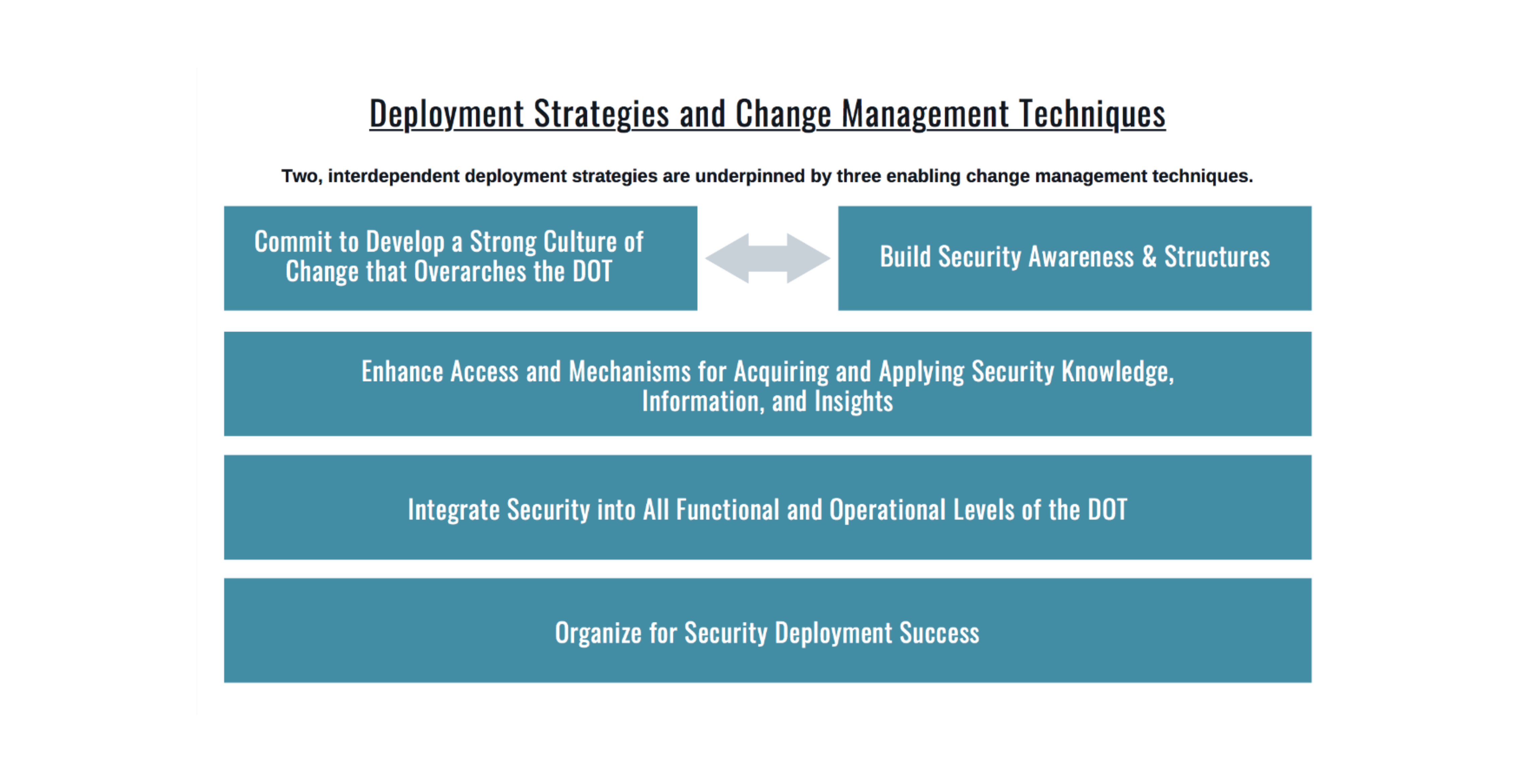
Deployment Strategies

Change Management Techniques

Security Implementation Tool

Security Parameters

Toolkits



Deployment Strategies and Change Management Techniques

Two, interdependent deployment strategies are underpinned by three enabling change management techniques.

Commit to Develop a Strong Culture of Change that Overarches the DOT

Build Security Awareness & Structures

Enhance Access and Mechanisms for Acquiring and Applying Security Knowledge, Information, and Insights

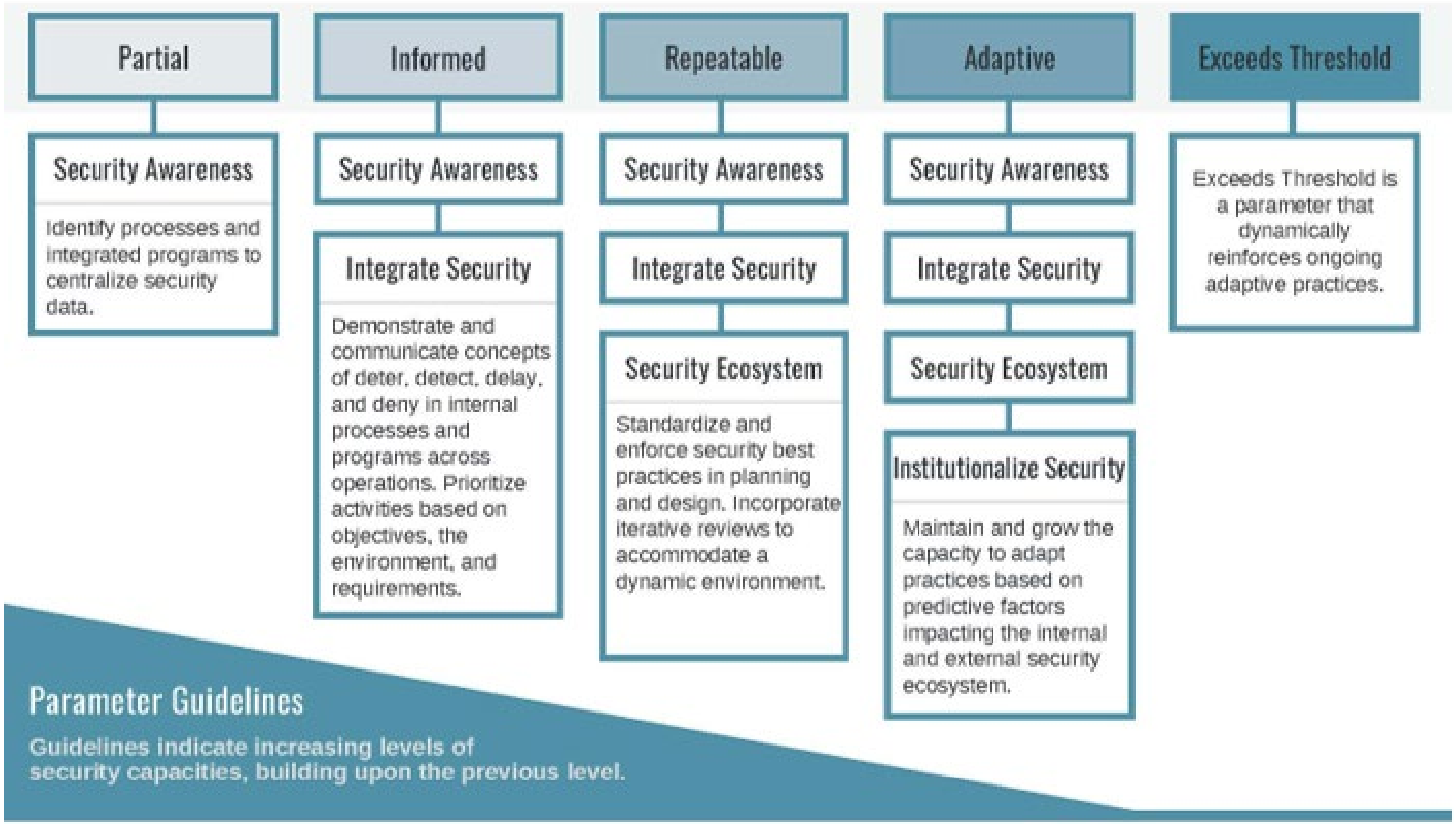
Integrate Security into All Functional and Operational Levels of the DOT

Organize for Security Deployment Success

Security Implementation Tool

An unbiased gateway connecting the deployment strategies, change management techniques, guidelines, and benchmarks

SECURITY PARAMETERS



Partial

Security Awareness

Identify processes and integrated programs to centralize security data.

Informed

Security Awareness

Integrate Security

Demonstrate and communicate concepts of deter, detect, delay, and deny in internal processes and programs across operations. Prioritize activities based on objectives, the environment, and requirements.

Repeatable

Security Awareness

Integrate Security

Security Ecosystem

Standardize and enforce security best practices in planning and design. Incorporate iterative reviews to accommodate a dynamic environment.

Adaptive

Security Awareness

Integrate Security

Security Ecosystem

Institutionalize Security

Maintain and grow the capacity to adapt practices based on predictive factors impacting the internal and external security ecosystem.

Exceeds Threshold

Exceeds Threshold is a parameter that dynamically reinforces ongoing adaptive practices.

Parameter Guidelines

Guidelines indicate increasing levels of security capacities, building upon the previous level.

Toolkits

Figure 7: DOT Annual Security Awareness Refresher

Delivery Technique: Interactive eLearning course

Description: The purpose of this module is to provide a review of basic security principles and responsibilities to protect DOT assets.

Terminal Learning Outcome: This course assesses and refreshes an employee's understanding of security policies and principles and their responsibilities to ensure the proper protection of DOT assets.

Enabling Learning Outcome: The employee may attempt this course an unlimited number of times. This course contains a pre-test as well as a post-test. You must receive a passing score (75%) on either the pre- or post-test to receive a certificate for this course.

Prerequisite: None.

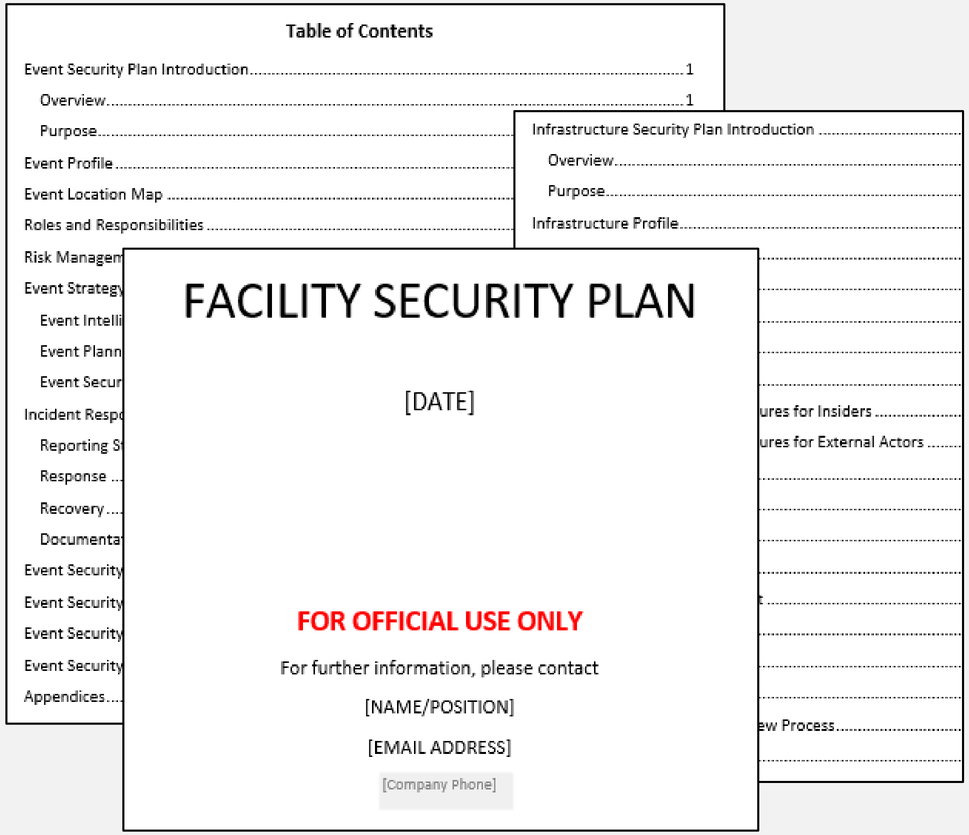


Table of Contents

FACILITY SECURITY PLAN

[DATE]

FOR OFFICIAL USE ONLY

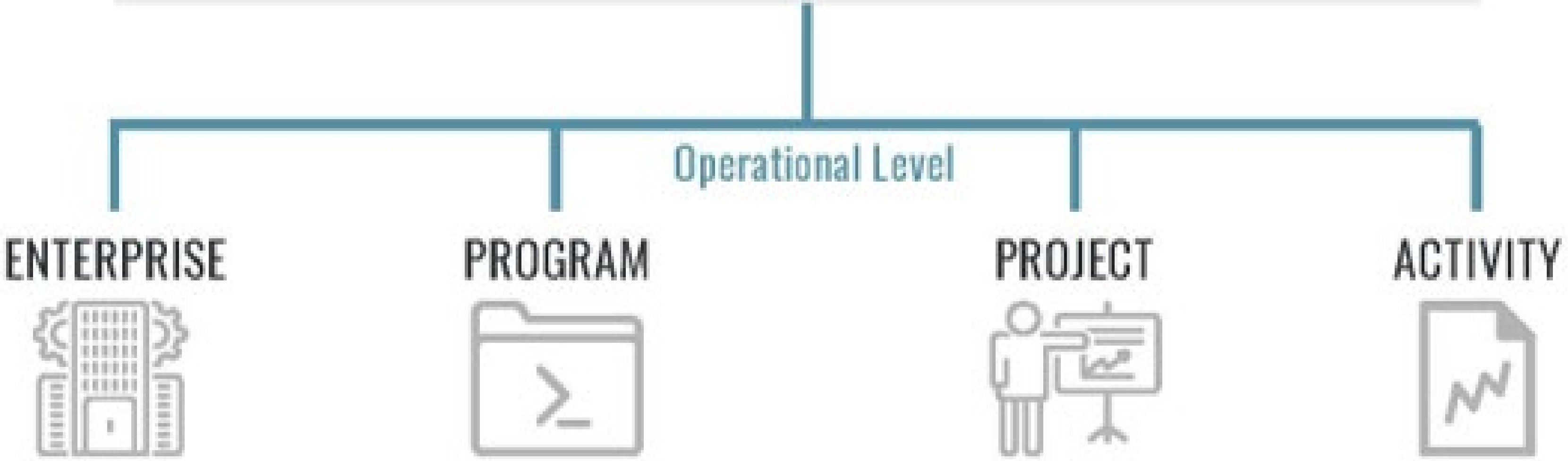
For further information, please contact

[NAME/POSITION]

[EMAIL ADDRESS]

[Company Phone]

Change management techniques aid leaders with deployment of security practices at four different operational levels



Security best practices for facility, infrastructure, and event-based components assist in the implementation at each operational level.

Facility
Event
Infrastructure

Actions & Outputs – Case Studies

Four case studies will provide data and insights on research at DOT or DOT-relevant levels. Case examples are provided in the Final Deliverable.

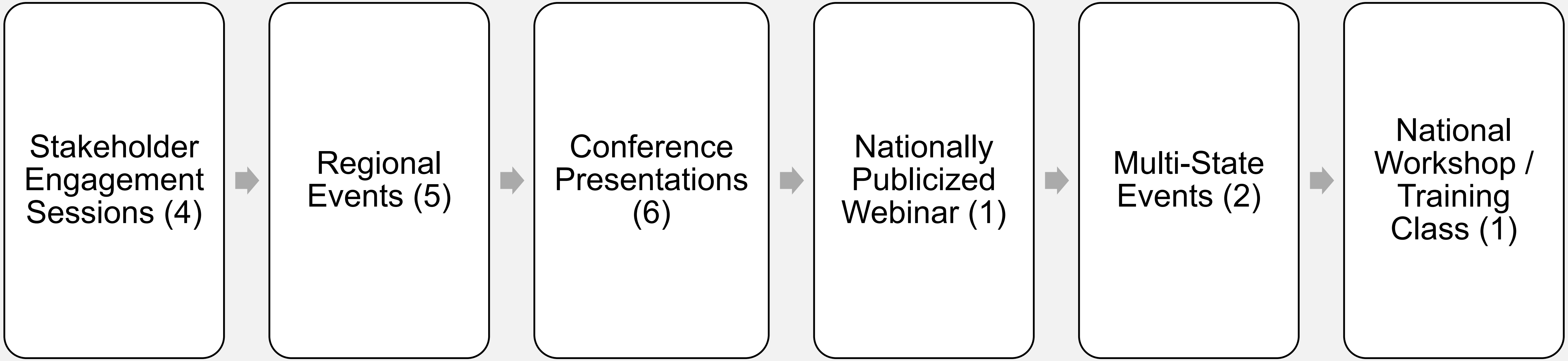
Components

1. Literature on models and frameworks for security did not include data or insights on use, outcomes, or levels of success. Case studies create this data and insights.
2. Peer-case examples to increase interest and widen the glide path for participation.
3. “How-to” examples of research implementation from various angles.

Cases

- MnDOT – 30-Month Research Progress (Michael Audino)
- Bridge Planning – Research to Practice (Dr. Jenni Hesterman)
- Cybersecurity – Research to Real-Time (Dr. Silvana Croope)
- ITD – Community Traction (Debbra Johnson)

Back to You!



Stakeholder Engagement Sessions (4)

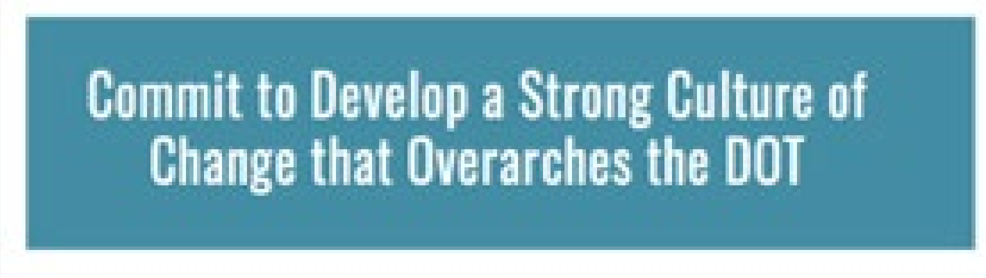
Regional Events (5)

Conference Presentations (6)

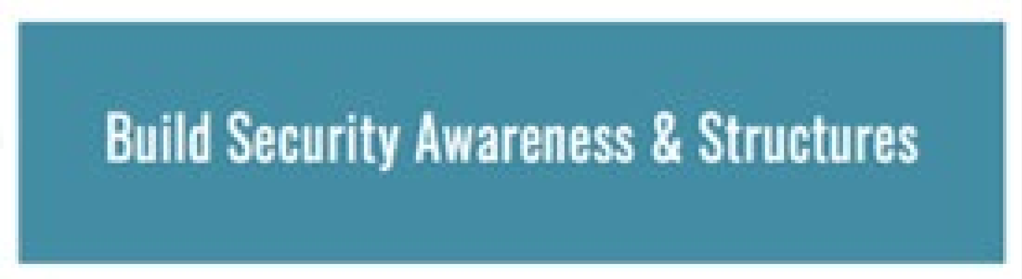
Nationally Publicized Webinar (1)

Multi-State Events (2)

National Workshop / Training Class (1)



Commit to Develop a Strong Culture of Change that Overarches the DOT

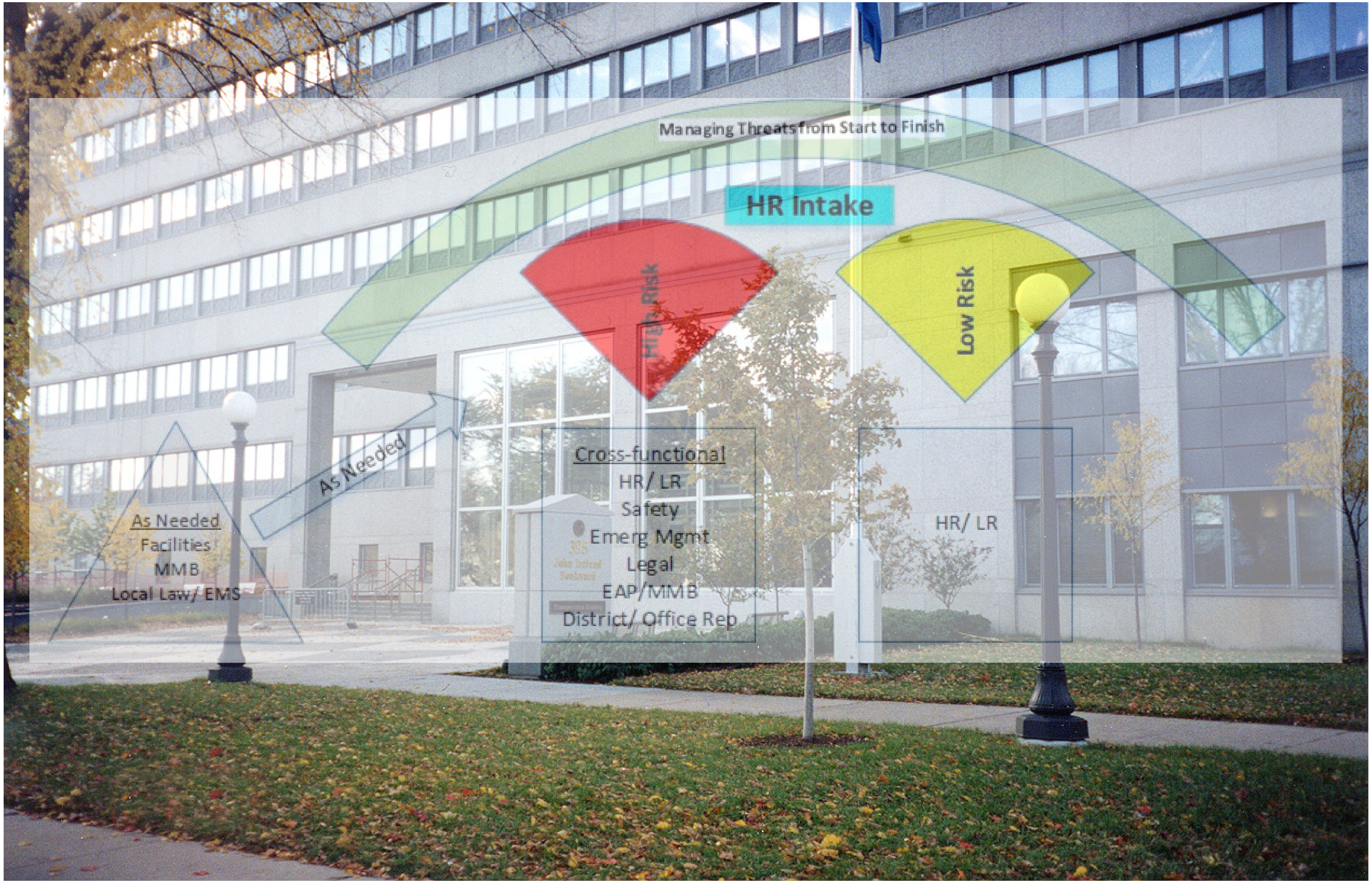


Build Security Awareness & Structures

Poll

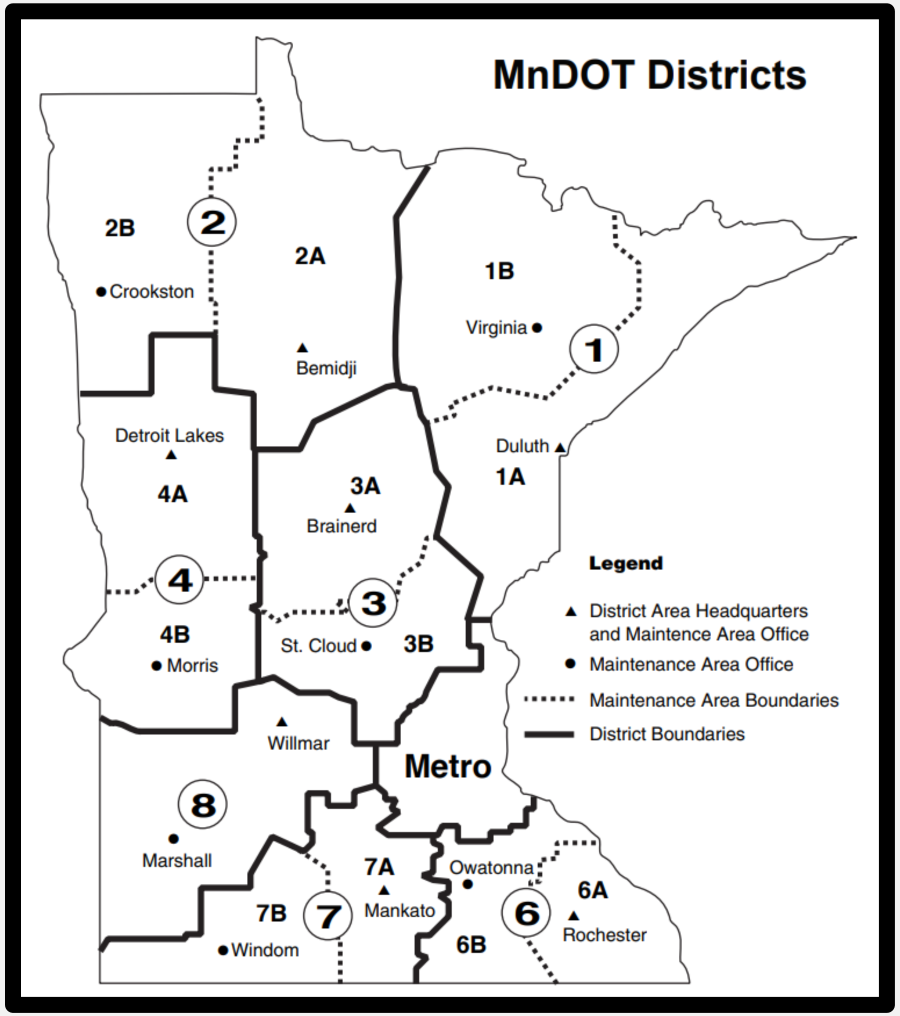
What part of the research will benefit your organization the most?

Minnesota Department of Transportation (MnDOT)



MnDOT At A Glance

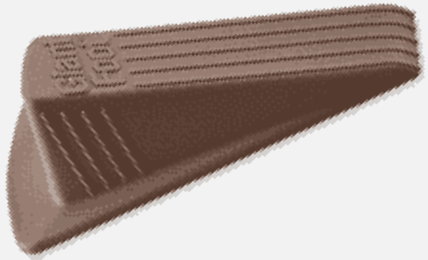
- >5000 employees over 85,000 square miles
- 150 occupied facilities
  - – Our largest is 1200
  - – Our smallest is 3
- 20,000 bridges
- >400 radio towers



Security @ MnDOT: Past

Well Meaning

- Ad hoc funded
- Leadership supported when they were asked to
- Equipment was purchased but not always maintained



"Doors propped open for convenience"

"Analog camera that went nowhere"

"Fleet management system"

Decentralized

- Inconsistent practices
- Budget and awareness-driven
- Little communication of trends, patterns, events statewide (siloes)

Security @ MnDOT: Present

My position is at the table with …

- Local LE
- HR and ADA
- EM, HSEM/CISA
- Leadership
- Financial mgmt.
- Long-term planning
- The modes
- Training (violent incident response, active shooter)

Visitor management system with easily identifiable ID badges

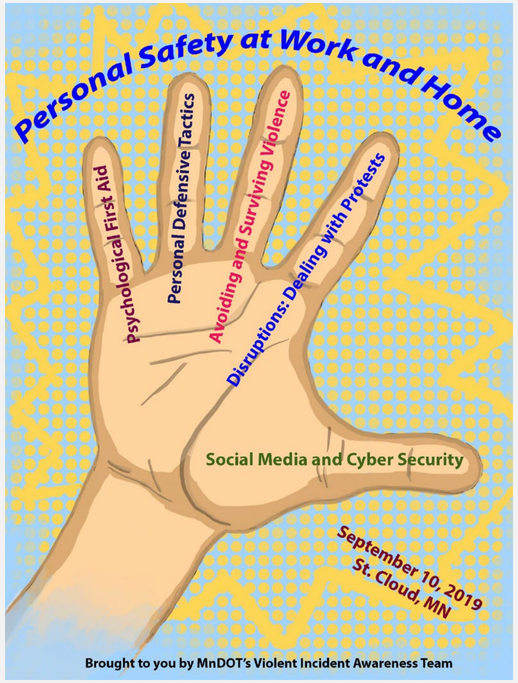

Personal Safety at Work and Home
Psychological First Aid
Personal Defensive Tactics
Avoiding and Surviving Violence
Disruptions: Dealing with Protests
Social Media and Cyber Security
September 10, 2019
St. Cloud, MN
Brought to you by MnDOT's Violent Incident Awareness Team

Photo by Jenny Seelen, District 3 Communications

Culture Change and the Need for Increased Security

Snow and Ice and "Minnesota Nice"

Secure AND accessible

Increasing security and difficult associations

Joshua Rashaad McFadden for The New York Times

Security @ MnDOT: Future

Seamless Integration of….

Administrative Controls

POLICY

PROCEDURES

CHECKLISTS

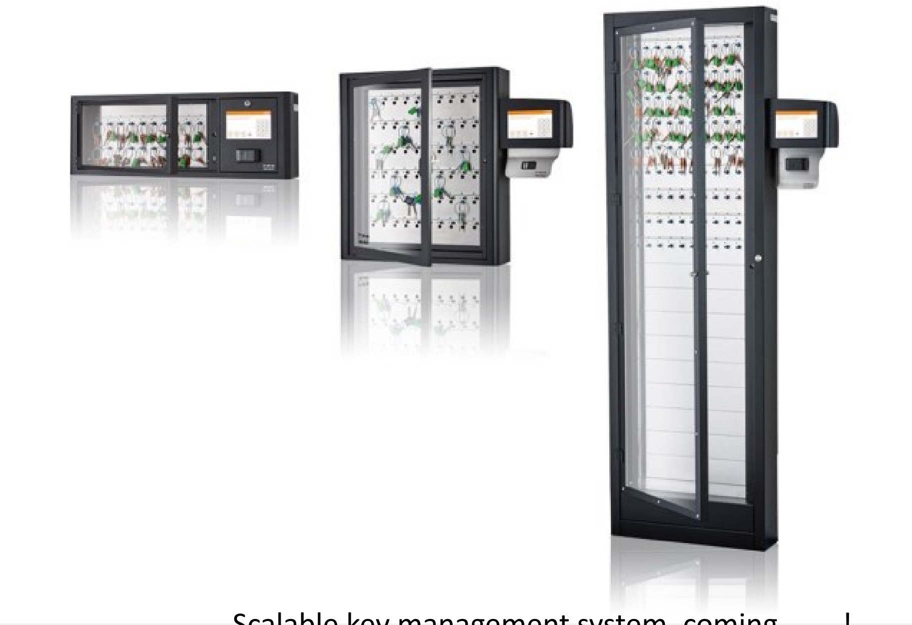
Education

Outreach

Collaboration

Empowerment

Engineering Controls

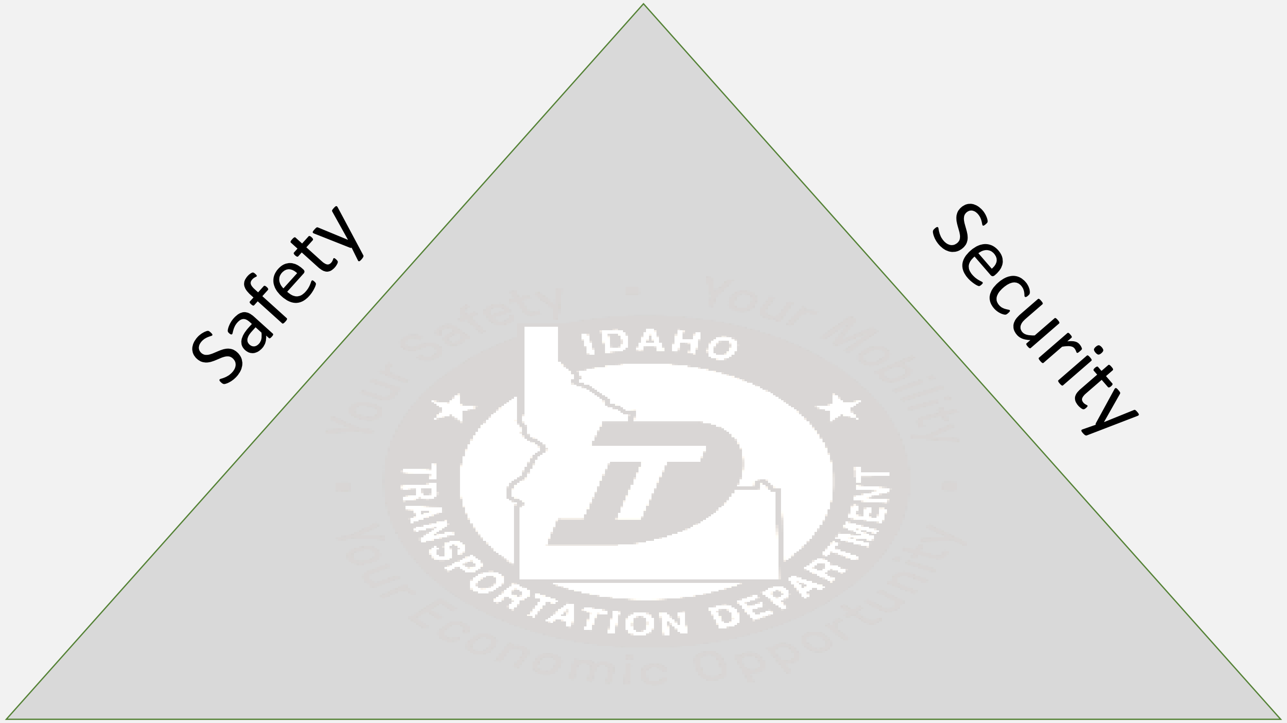


Scalable key management system, coming____!

Boon Edam turnstiles, coming July 2021!26B

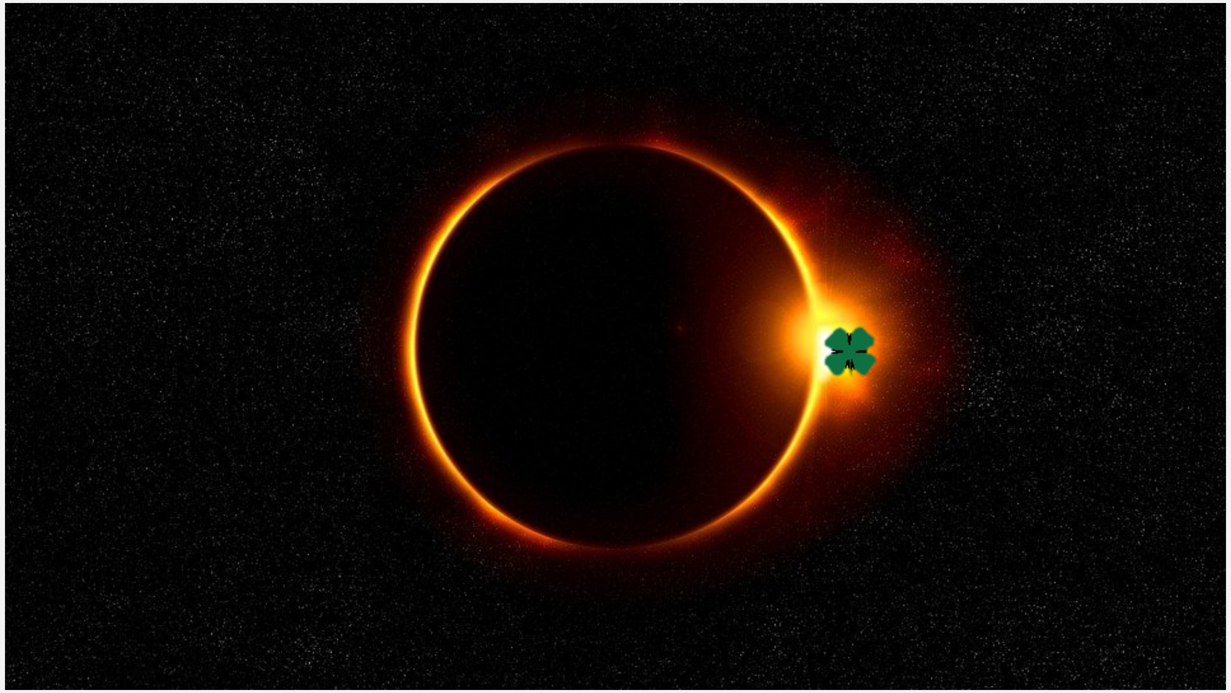
Idaho Transportation Department (ITD)

ITD Advances Security



Safety
Security
IDAHO
TRANSPORTATION DEPARTMENT
Your Safety • Your Mobility • Your Economic Opportunity

Preparedness



In the beginning

God Created the Irish

And with it came

Murphy's Law of Security

Experience is something you don't get until after you need it!

Now the rest of the story

9-11 to Sleepy Hollow then a “Tipping Point (s)”

- Threat Hazard Identification Risk Analysis
    - Growth, Crime, Situational Awareness
  - Constitutionalist
    - Video
  - Headquarters Caller -Director
  - Cyber
    - Attack(s)
- Prepared not Paranoid

Team Work - Internal

- Communication
  - HSIN/Fusion Center
  - EMR-ISAC
- Shortened Checklist
  - Easy for quick reaction
- Employee teams
  - Security, Emergency, Employees as sensors
- Security Incident Tracking
  - Do we have an issue?
- Cyber
  - Team with Emergency Manager - Incident (EOC)

Standard procedures for every Building/Section/District

Open but secure

Facility Management

Security Plan

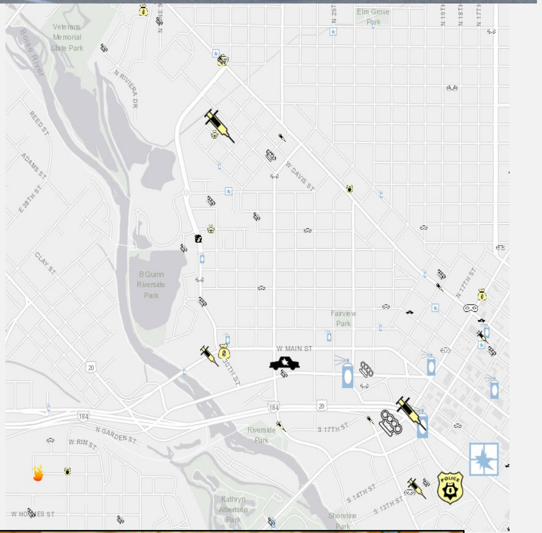
Development/Strengthen

Implementation

SAFE
SECURE
PREPARED

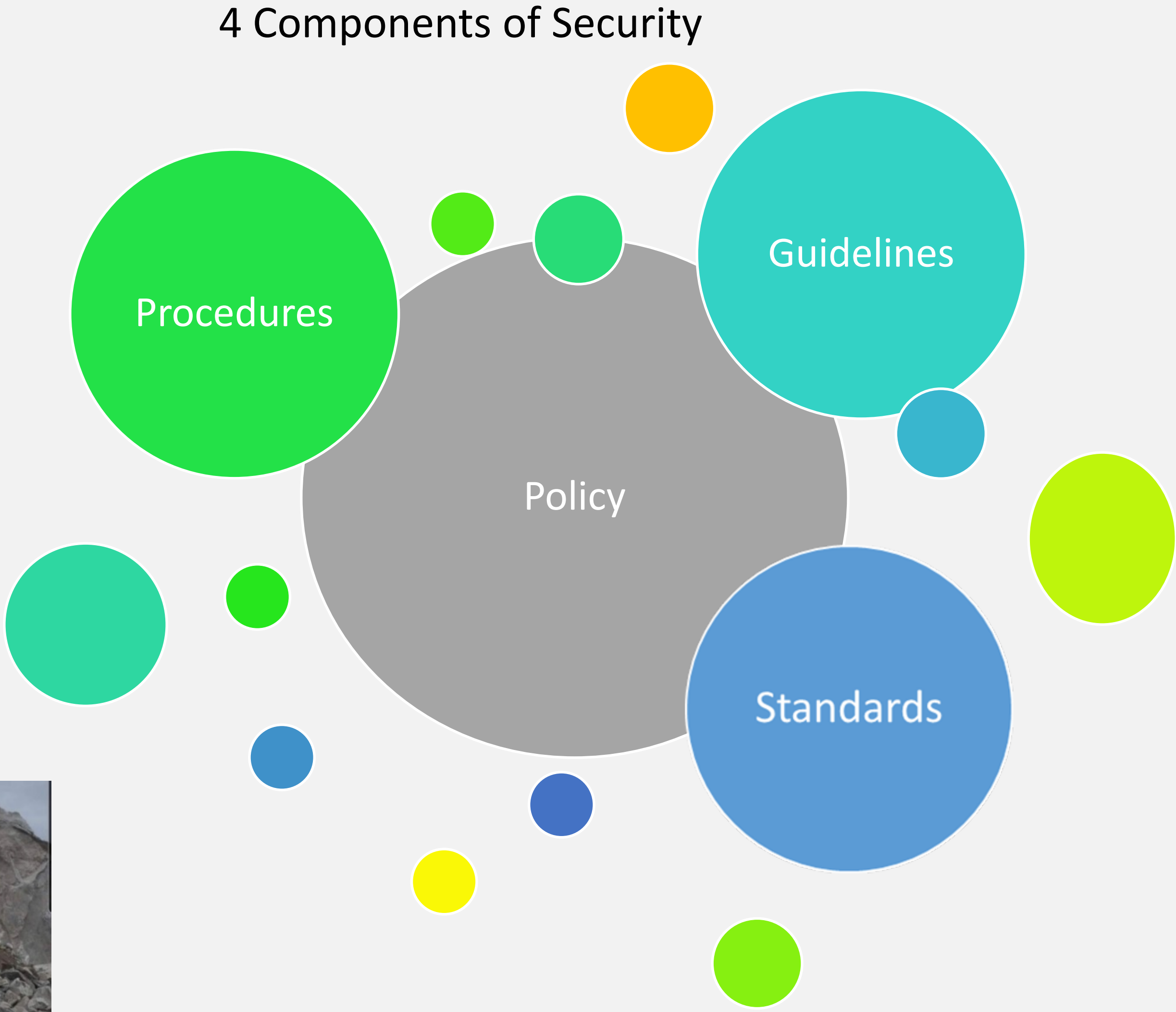
Team Work - External

- Department of Homeland Security
    - Active Assailant Training Exercise
    - Facility Security review
        - D1/2
        - HHQ
- Local and State Agencies
    - Coordination with
        - Office of Emergency Management
        - National Guard
        - Health and Welfare
        - Local LE/FIRE
        - Idaho State Police

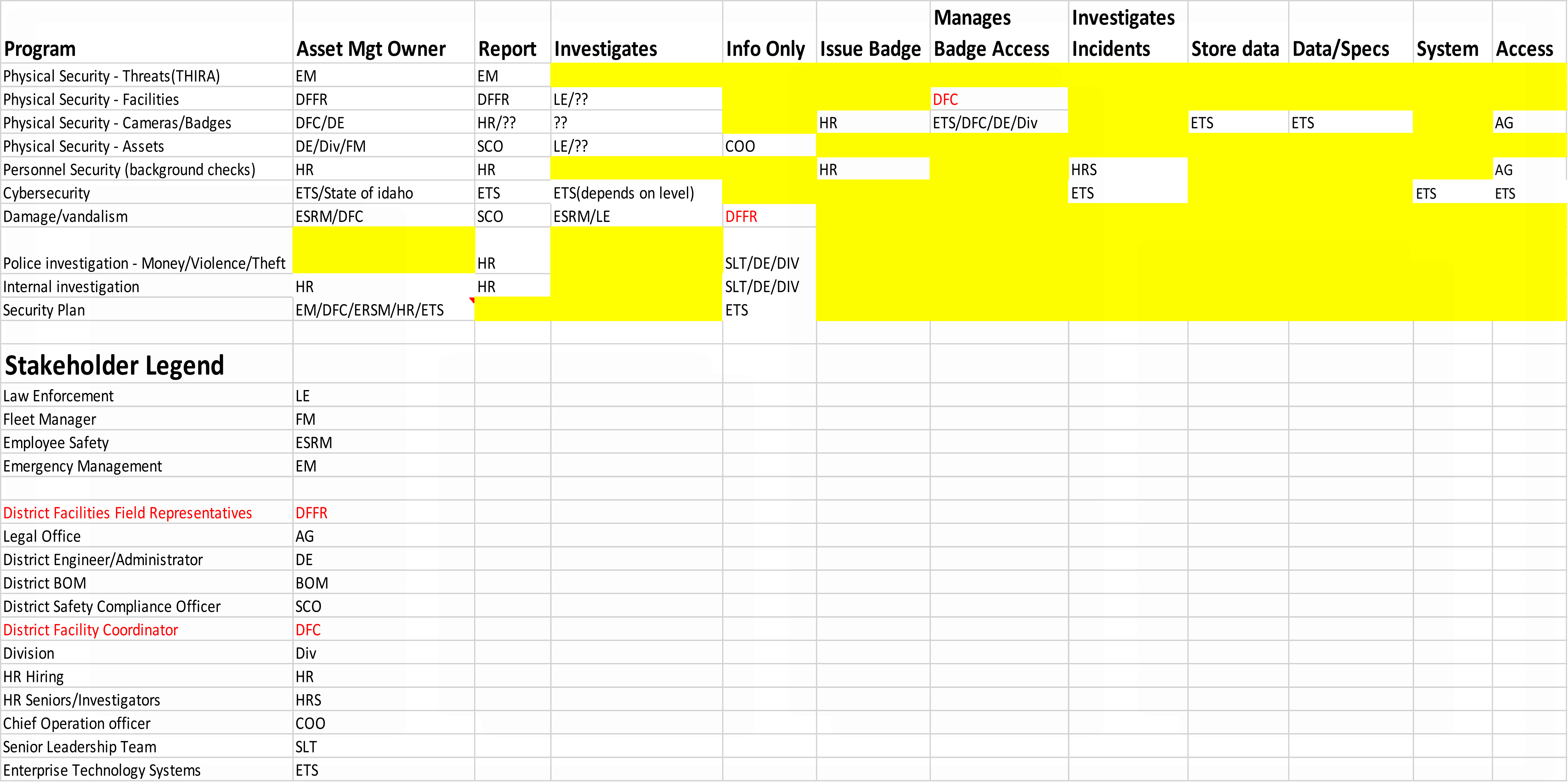


Small rocks in the way of security

Access/Security
Door
  Gates
  Badges
Cameras
Emergency Apps
Cyber
Facilities
Alert Sense
HR actions
Mail
Exercise/Drills
Communication with LE/Fire/EMS



Who does what for security?



Program	Asset Mgt Owner	Report	Investigates	Info Only	Issue Badge	Manages Badge Access	Investigates Incidents	Store data	Data/Specs	System	Access
Physical Security - Threats(THIRA)	EM	EM									
Physical Security - Facilities	DFFR	DFFR	LE/??			DFC					
Physical Security - Cameras/Badges	DFC/DE	HR/??	??		HR	ETS/DFC/DE/Div		ETS	ETS		AG
Physical Security - Assets	DE/Div/FM	SCO	LE/??	COO							
Personnel Security (background checks)	HR	HR			HR		HRS				AG
Cybersecurity	ETS/State of idaho	ETS	ETS(depends on level)				ETS			ETS	ETS
Damage/vandalism	ESRM/DFC	SCO	ESRM/LE	DFFR							
Police investigation - Money/Violence/Theft		HR		SLT/DE/DIV							
Internal investigation	HR	HR		SLT/DE/DIV							
Security Plan	EM/DFC/ERSM/HR/ETS			ETS							

Stakeholder Legend

Law Enforcement	LE
Fleet Manager	FM
Employee Safety	ESRM
Emergency Management	EM
District Facilities Field Representatives	DFFR
Legal Office	AG
District Engineer/Administrator	DE
District BOM	BOM
District Safety Compliance Officer	SCO
District Facility Coordinator	DFC
Division	Div
HR Hiring	HR
HR Seniors/Investigators	HRS
Chief Operation officer	COO
Senior Leadership Team	SLT
Enterprise Technology Systems	ETS

Policies

- 4059 – ITD System and Information Security
- 5059
- 0616
  - Security Access Procedures 2016 - Draft
  - Background Check Committee 2016 – Draft
  - Velocity Tiger Team 2021 -Working
  - Training links and schedule – State wide

Ride the wake

Constant movement adjusting to the motion of the wake-- always learning, changing and adapting to take our organization to a more secure, safe and ready state.

Poll

What are your greatest security challenges?

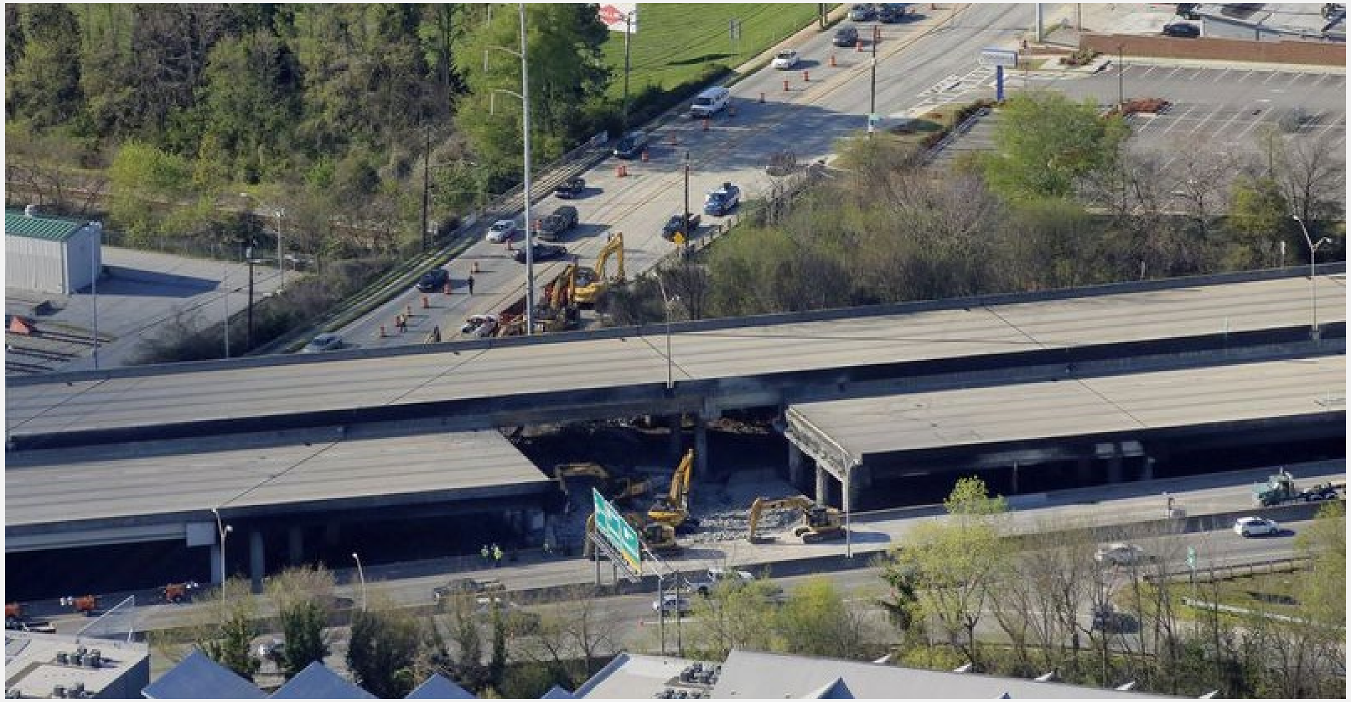
Case Study: Bridges

Bridges: Critical and Vulnerable Infrastructure

- 618,456 bridges in the U.S. critical to moving people and goods
- 45,031 bridges are rated "poor"; 19 carry 200,000+ vehicles a day
- 918 bridges are rated "Scour Critical" due to flood erosion around piers and abutments; immediate countermeasures required
- Vulnerable to escalating extreme weather events - flooding, surge, wildfires
- In addition to ratings and age, public websites and documents contain detailed data on design, construction, repairs, vulnerabilities, et al

Sources: InfoBridge, bridge deck preservation reports, load posted bridge databases

Atlanta I-85 Bridge Collapse



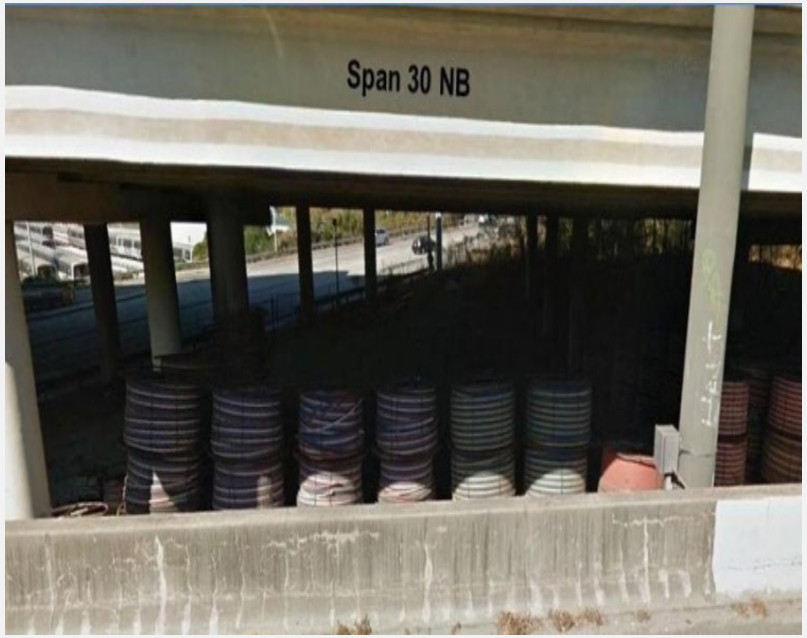
"Most bridges constructed of steel and concrete are inherently fire resistant and have a relatively low risk of being seriously damaged by fire." NTSB/HAB-18/02

March 30th, 2017

- 6:05 PM: A man under the bridge purposely ignites a chair atop unsafely stored high-density polyethylene and fiberglass conduit (NTSB)

- Hazardous materials ignite, the structure catches fire; law enforcement clears the bridge above

- 7:14 PM: A 92-foot-long section collapses



NTSB/HAB-18/02

Impact

- A 3-mile portion of I-85 is closed, a major artery running through the heart of Atlanta

- Governor declares a State of Emergency, delayed openings for government offices and approval to telecommute

- Bridge carried 250,000 vehicles a day; MARTA system flooded with 25% increase in ridership

- Commuters took alternative routes, saturating other highways and local roads

Response and Recovery

- GA DOT coordinates response efforts with the Department of Public Safety, Georgia Emergency Management and Homeland Security Agency

- Inspects all bridges in the state, revamps GDOT procedures regarding storage under bridge and other structures

- Five spans adjacent to the collapse also replaced; new span constructed in 43 days at a cost of $15 million

Bridge Fire Data

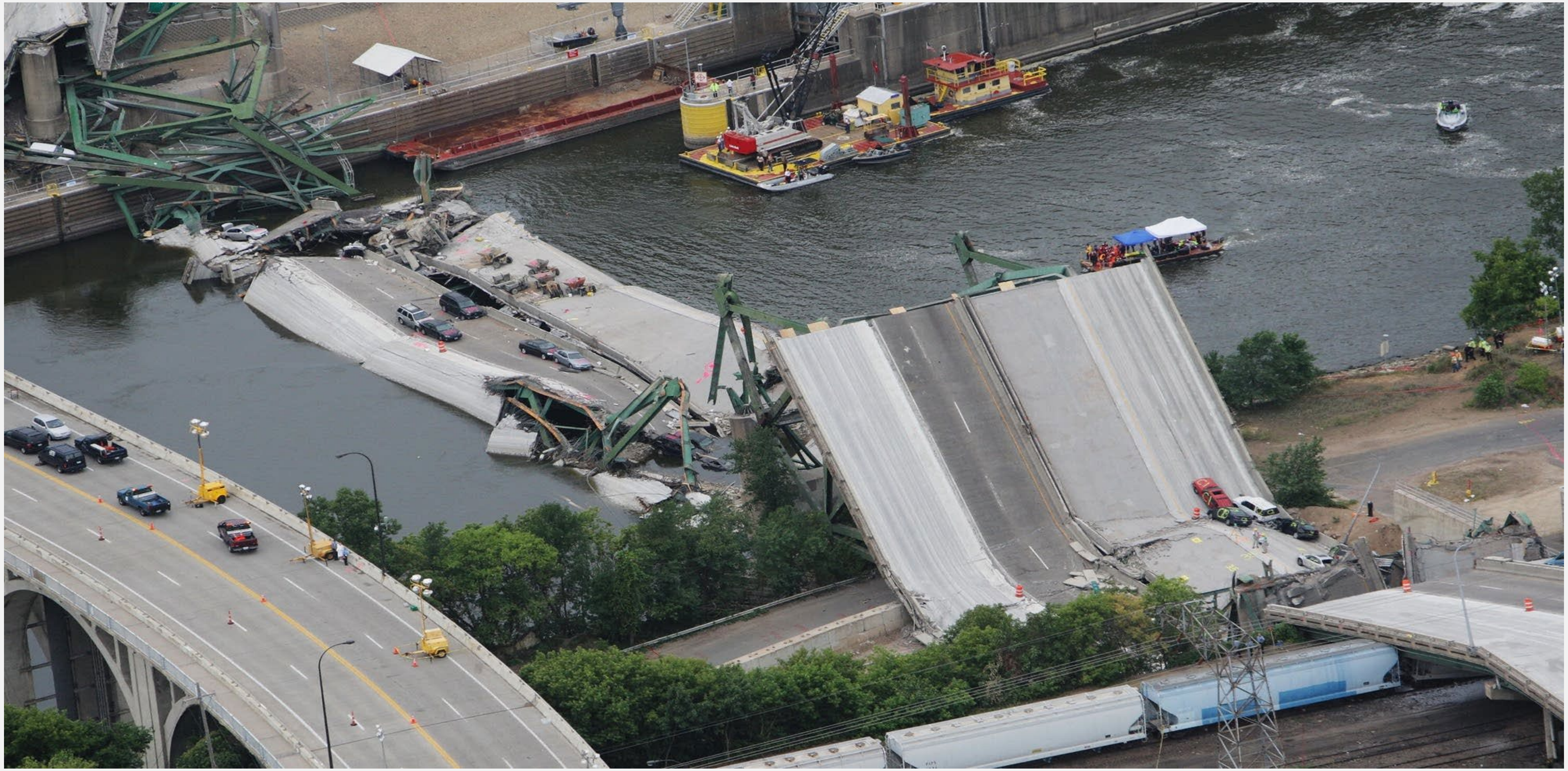
- Studies reviewed 165 fires on or near bridges from 1997 - 2015

- Nine steel structures and 15 wooden ones collapsed; 35 others were damaged so badly they had to be replaced

  - 2004: I-95 collapse in Connecticut, car struck a fuel tanker
  - 2007: MacArthur Maze interchange in California collapse, fuel tanker below caught fire
  - 2009: I-75 collapse in Michigan, 3-vehicle collision with fuel tanker

Sources:
Fire Hazard in Bridges: Review, Assessment and Repair Strategies (2012)
Detailed Analysis of the Causes of Bridge Fires and Their Associated Damage Levels (2017)

Minneapolis I-35 Bridge Collapse



August 1, 2007

- I-35W Mississippi River bridge was an eight-lane, steel truss arch bridge carrying 140,000 vehicles daily

- Collapsed during evening rush hour, killing 13 and injuring 145

- NTSB: design flaw likely cause; a too-thin gusset plate ripped along a line of rivets; extra weight from paving vehicles also contributed

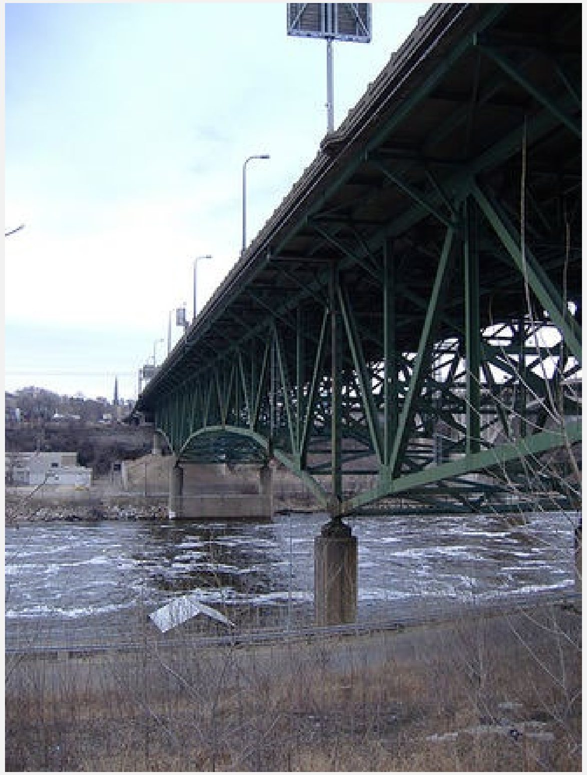
- Inspections found over 100 bridges in the state lacking key design redundancies; they were retrofitted or replaced

- Bridge replacement cost - $234 million

Compounding Risk

1990: Bridge rated "structurally deficient" due to significant corrosion in its bearings
2001: Study finds cracking in the girders
2005: Bridge again rated "structurally deficient"
2006:

- A steel reinforcement project is planned, but canceled in favor of periodic safety inspections since drilling might weaken the bridge
- Officials worry about the possibility of the bridge collapsing, impact of condemning it, cost to replace



I-35W Bridge seen from below in 2006

Human-Driven Events

2002: I-40 in Oklahoma, a barge collides with a pier causing a section of I-40 bridge to collapse, killing 14

Jeff Mitchell / Reuters

2002: Rafiganj rail bridge in India collapses, train falls into the river killing 130; political extremist group removed "fish plates" anchoring the rails to the bridge

2012: Jernbanebroen over Limfjorden rail bridge struck by a ship due to communication error; closed for a year

Other collapses due to faulty demo processes, construction errors, cutting corners, cheap materials

Bridges are Attractive Targets

Why?

- Symbolic targets
- Critical transportation modes; economic impact
- Well-timed attack could lead to mass casualties
- Stress transit system for later attacks
- Inflict fear/doubt in populace, gain press coverage, legitimize the group

The consequences of terrorist attacks are never unidimensional

Who?

- International and domestic terrorists – right, left, religious, single issue
- Insiders who are hostile, radicalized, or incentivized

Bridge Attack Data

How?

- Since 1975, at least 725 terrorist attacks were perpetrated on bridges and tunnels worldwide, many by the same groups threatening the U.S.

- Explosive devices/material used in 678 attacks; Firearms (26), Incendiary (17)

"Preliminary studies indicate there are approximately 1,000 bridges in the U.S. where substantial casualties, economic disruption, and other societal ramifications would result from isolated attacks."
(2003 Blue Ribbon Panel on Bridge and Tunnel Security)

Source: Why Terrorists Do Not Attack US Bridges and Tunnels: A Preliminary Investigation, 2017

Bridges are Attractive Targets

Past plots and ideations give insight...

- Brooklyn Bridge, George Washington Bridge, Tampa and Utah plot
- Anarchist: attempt to drop a bridge in Cleveland using C-4
- AQ provided training on “methods to destroy suspension bridges"
- Crude attacks such as two bridges in London and NYC bike trail attack - planned to continue onto the Brooklyn Bridge pedestrian path

Use of Imagination Critical in Security

9/11 Commission Report, Chapter 11, “Foresight—and Hindsight.”

- Investigators cite a lack of imagination as a root cause of the two worst attacks in our country’s history: Pearl Harbor and 9/11

- "Imagination is not a gift usually associated with bureaucracies"

- “It is therefore crucial to find a way of routinizing, even bureaucratizing, the exercise of imagination."

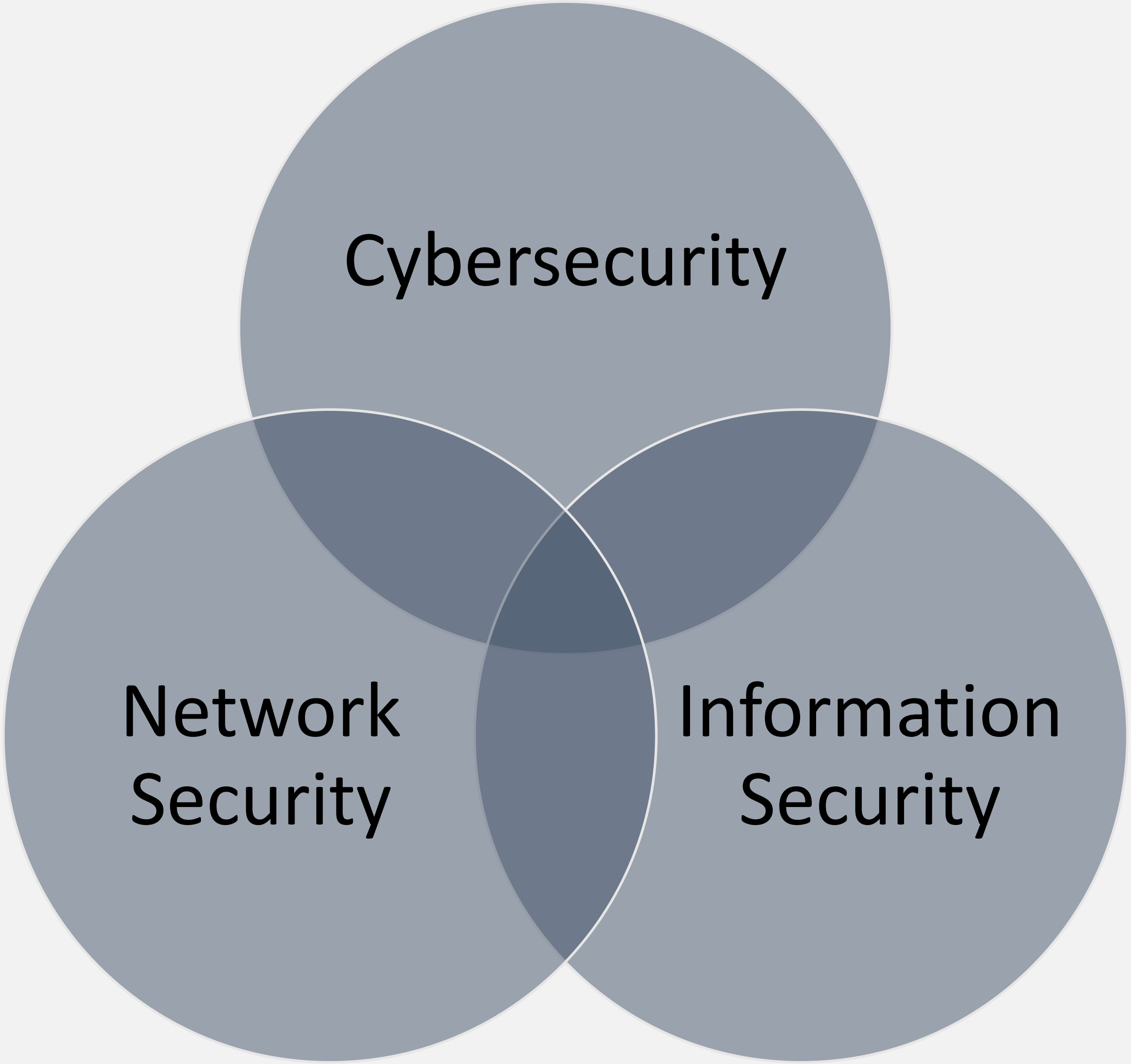
What Can We Do?

- Don't underestimate the sophistication of bad actors
- Understand we don't dictate the target list
- "Not seen" doesn't mean "not there"
- Strongly consider insider threat - fight "NIMO" - Not in My Organization
- Safeguard documents and data which could serve as a target list
- Harvest case studies on past attacks/plots to inform security practices
- Actively harden targets
  - Use security language on websites and signage
  - Deter, offroad - make it look too hard for those sizing up the target

Remember: The best offense is a good defense!

Case Study: Cybersecurity

The Digital Age



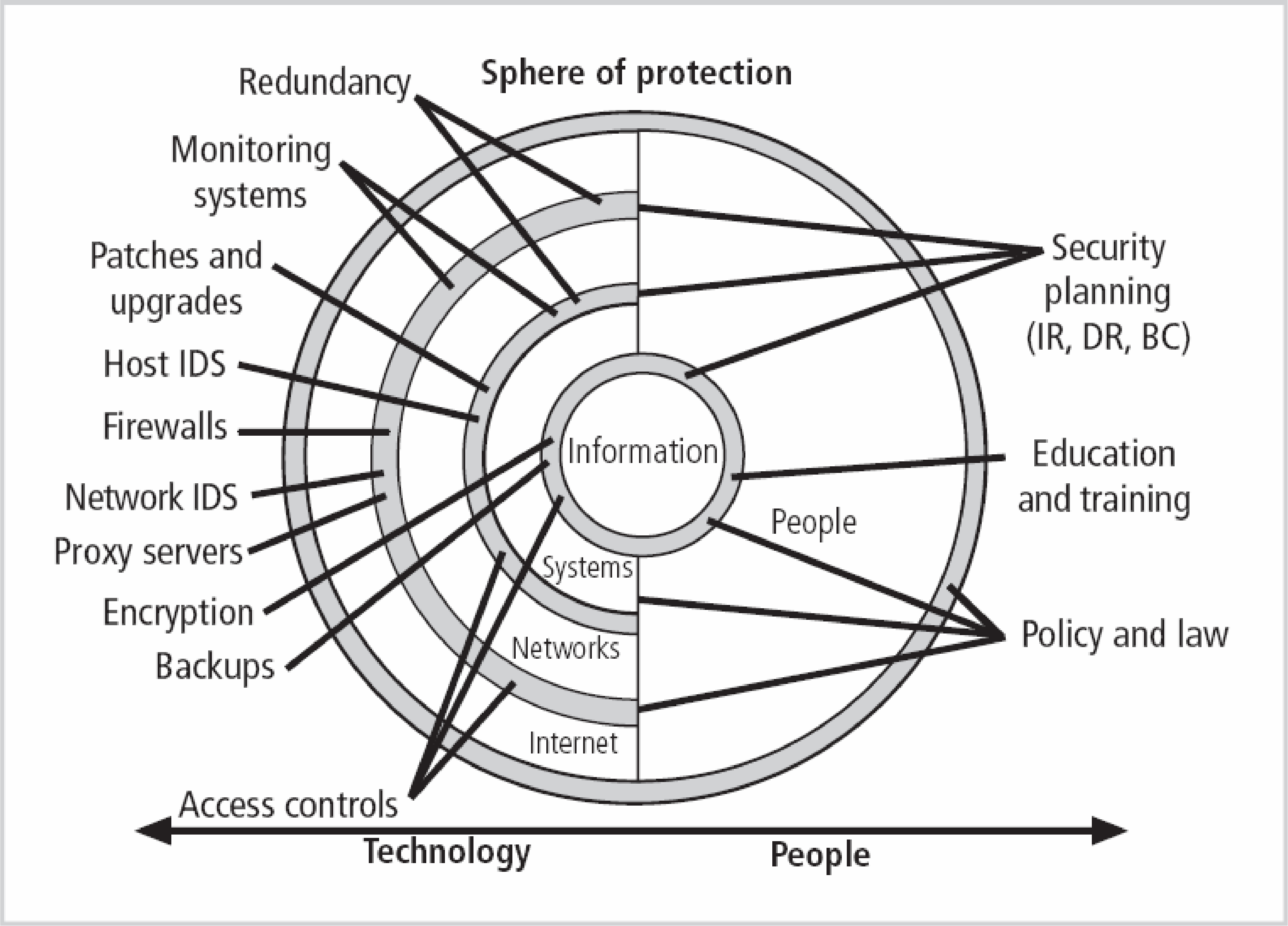
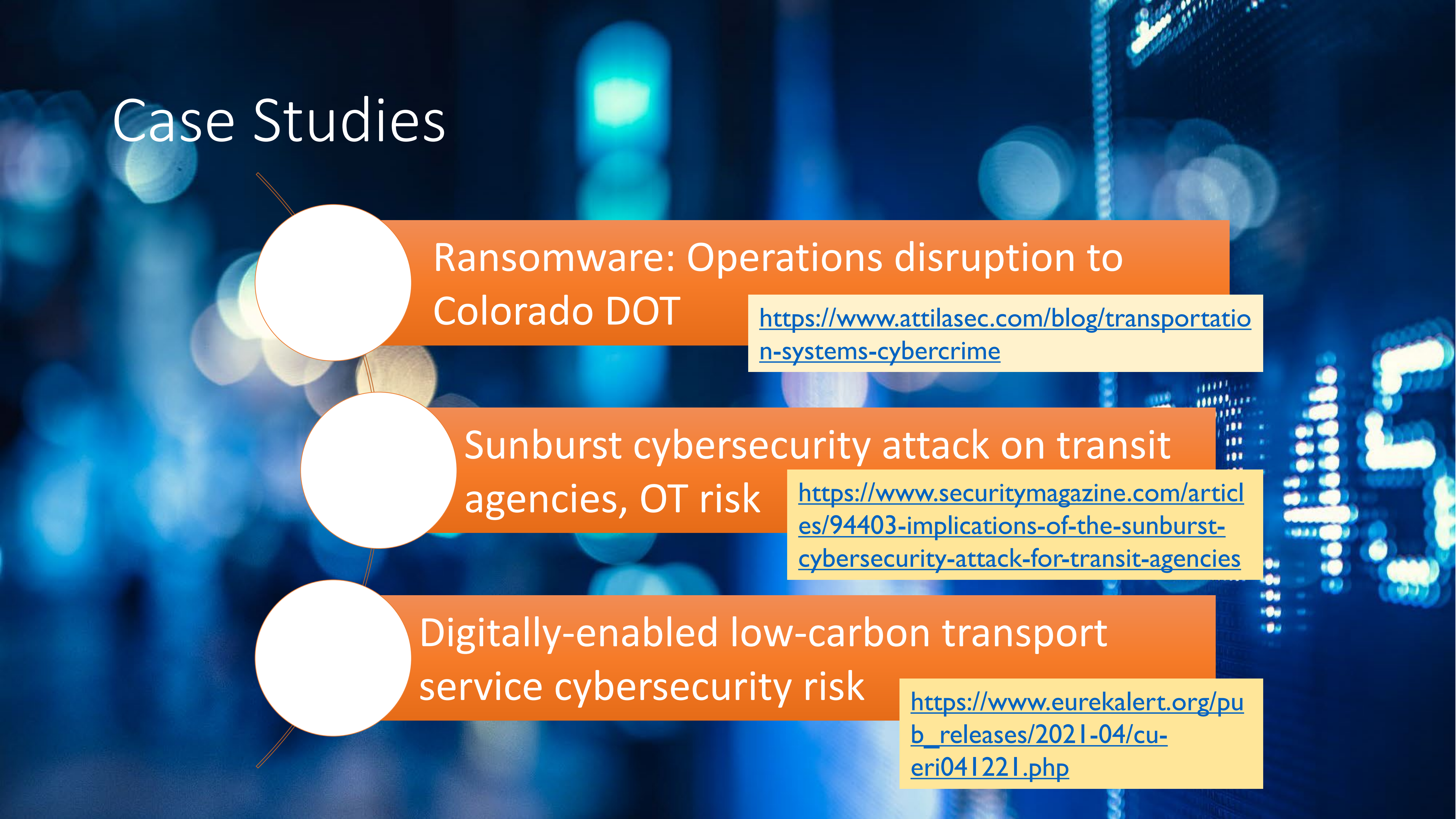


FIGURE 9-1 Sphere of Security

Source: Management of Information Security, 2nd ed. - Chapter 9



Case Studies

- Ransomware: Operations disruption to Colorado DOT

  https://www.attilasec.com/blog/transportation-systems-cybercrime

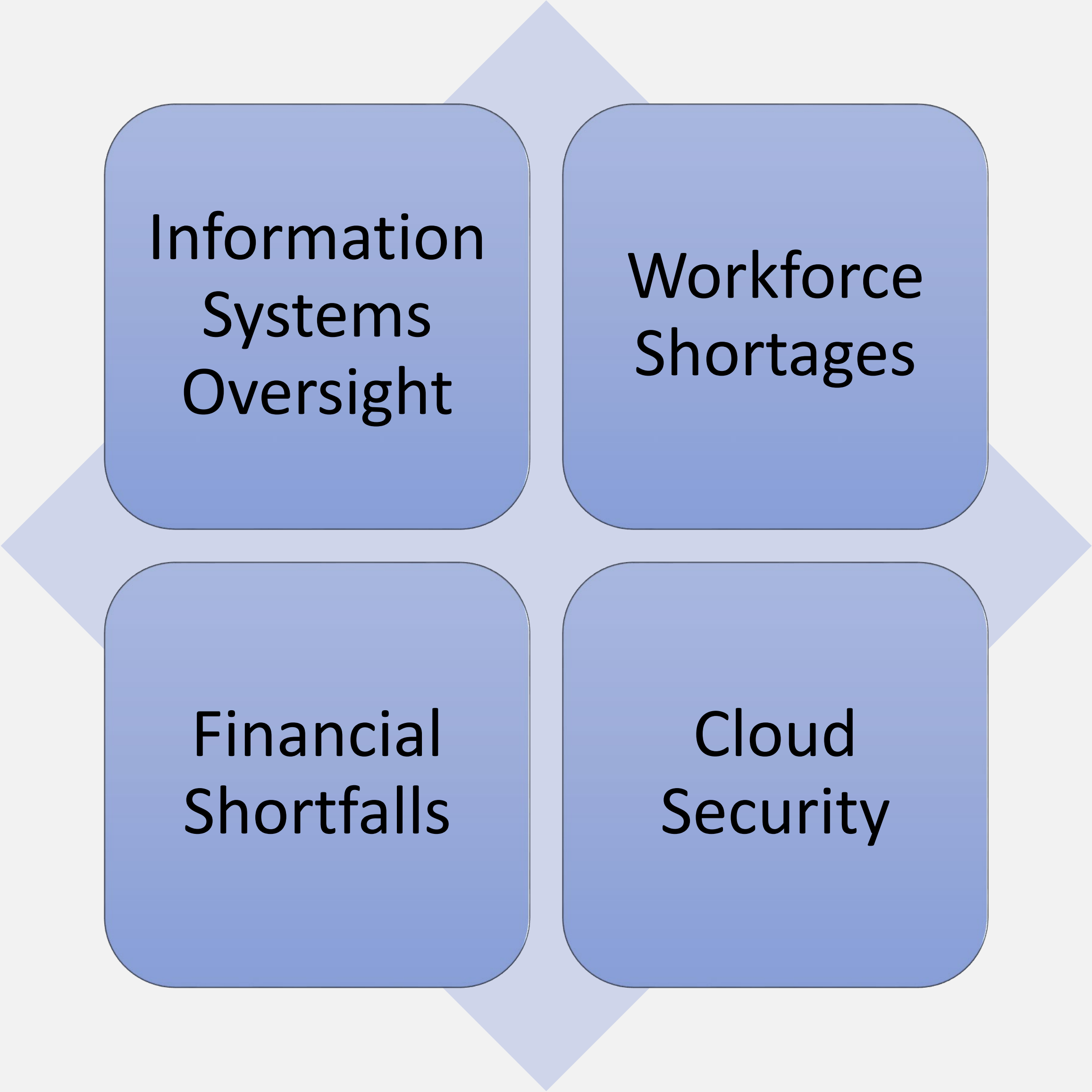
- Sunburst cybersecurity attack on transit agencies, OT risk

  https://www.securitymagazine.com/articles/94403-implications-of-the-sunburst-cybersecurity-attack-for-transit-agencies

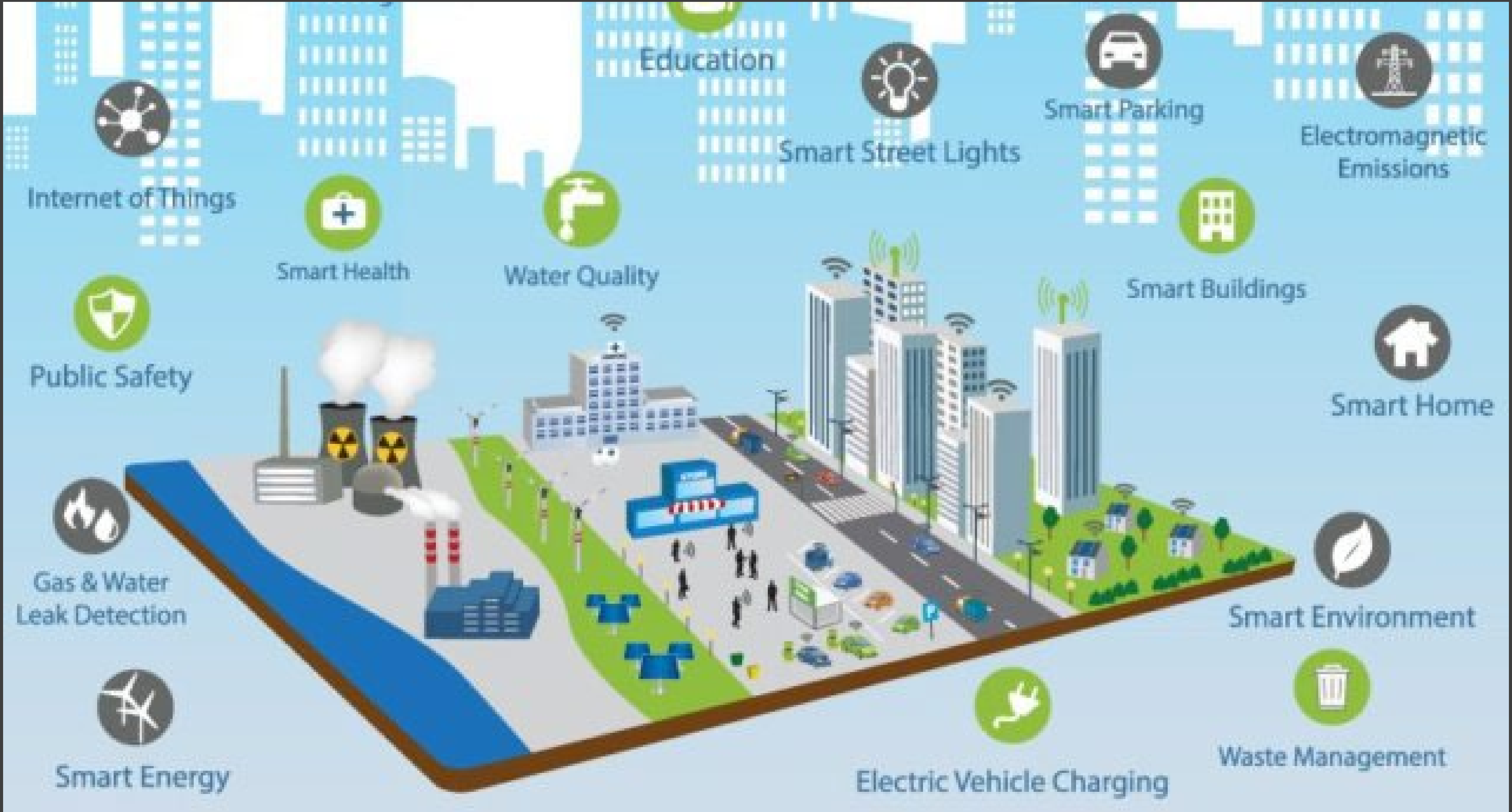
- Digitally-enabled low-carbon transport service cybersecurity risk

  https://www.eurekalert.org/pub_releases/2021-04/cu-eri041221.php

Challenges Await



Sources:
Bielby, Kylie. (2020, October 24). *What Are the Top Security Challenges for U.S. Transportation?* Government Technology & Services Coalition's Homeland Security Today. US. https://www.hstoday.us/subject-matter-areas/airport-aviation-security/what-are-the-top-security-challenges-for-u-s-transportation/.
Gehlhaus, Diana. (2021, April 9). *The Reality of America's AI Talent Shortage.* The Hill. https://thehill.com/opinion/technology/547418-the-reality-of-americas-ai-talent-shortages.



Source: https://internetofbusiness.com/global-smart-city-platform-market/

Why you are here.

Learn how to incorporate security practices into daily activities – become a force multiplier.

Share thoughts and concerns on security in the workplace and receive feedback from experts in the field.

Become part of a community influencing changes to security thinking in transportation.

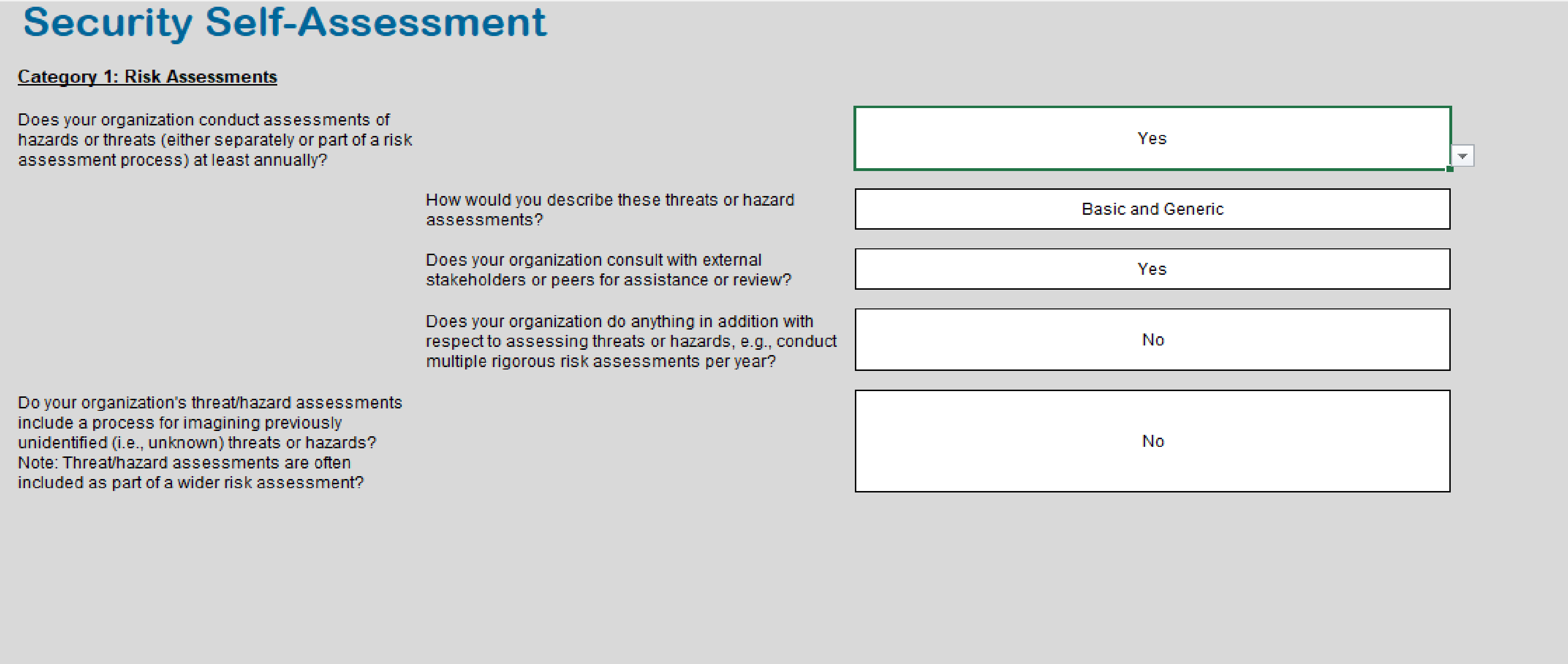
Make the lives of the people that we serve better.

Best Practices

- Leverage technology
- Begin with the end in mind

Security Implementation Tool

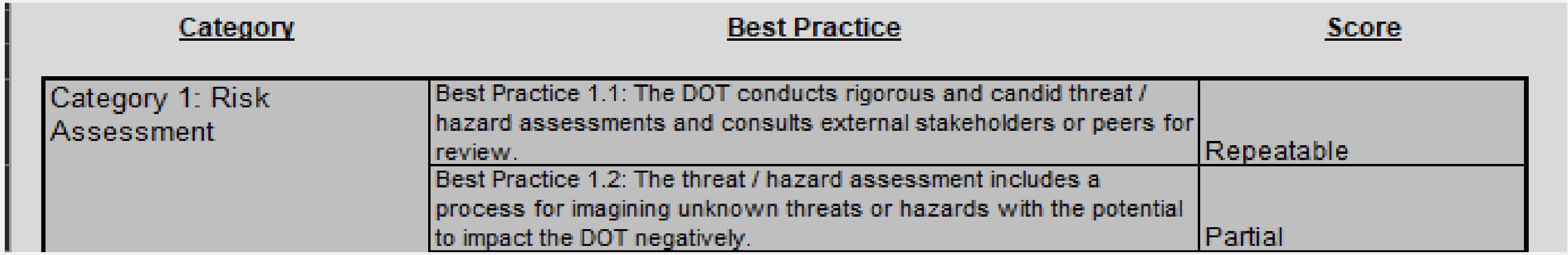
Components



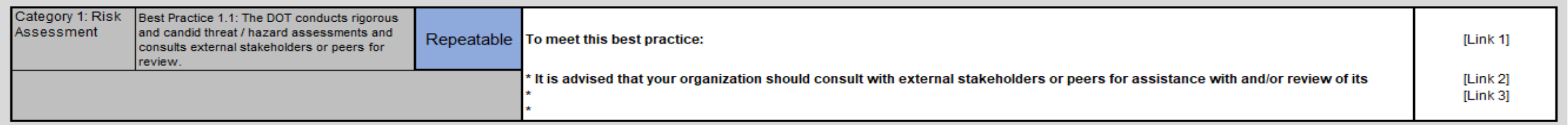
Security Self-Assessment

Category 1: Risk Assessments

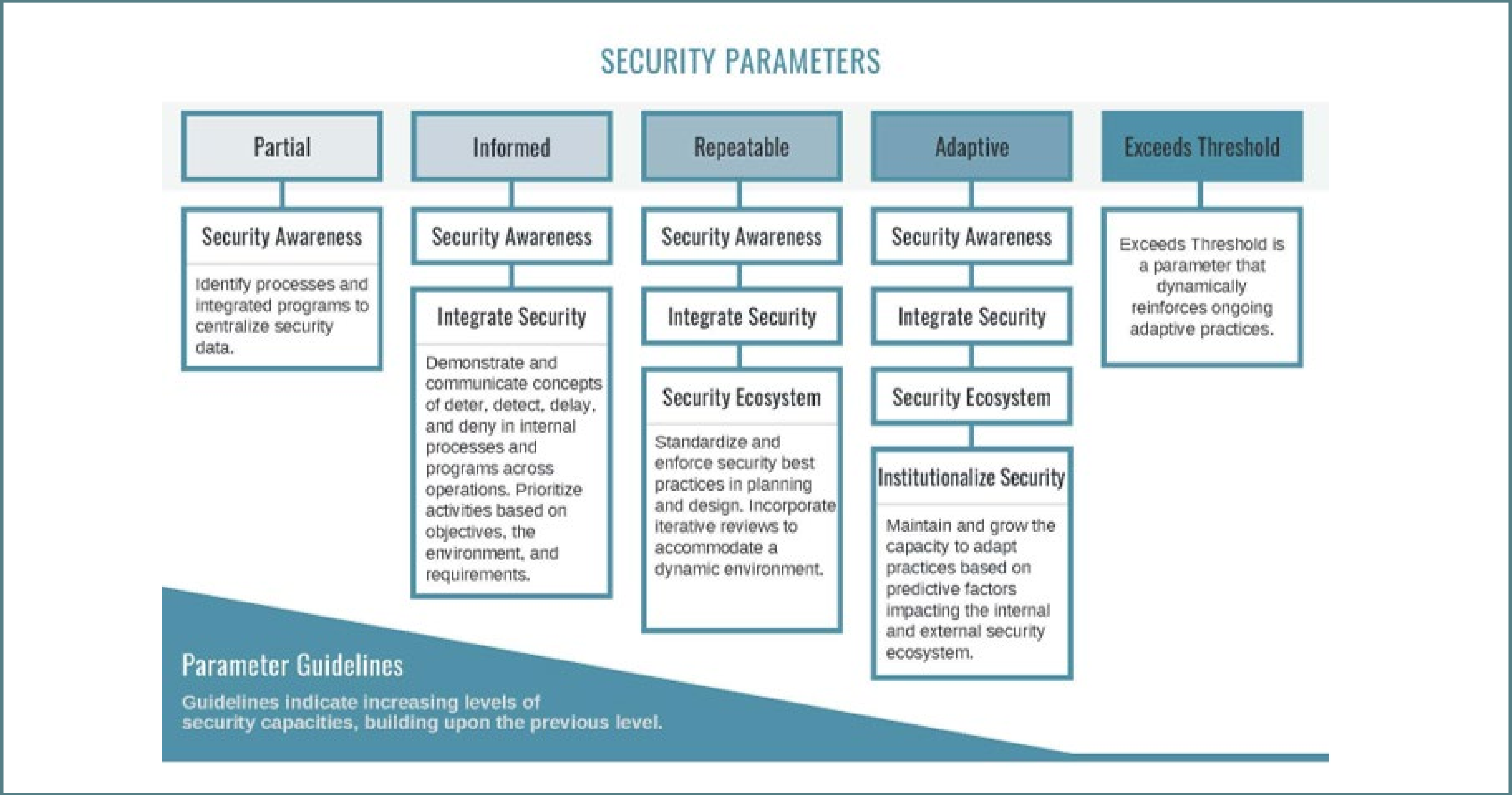
Does your organization conduct assessments of hazards or threats (either separately or part of a risk assessment process) at least annually?	Yes
How would you describe these threats or hazard assessments?	Basic and Generic
Does your organization consult with external stakeholders or peers for assistance or review?	Yes
Does your organization do anything in addition with respect to assessing threats or hazards, e.g., conduct multiple rigorous risk assessments per year?	No
Do your organization's threat/hazard assessments include a process for imagining previously unidentified (i.e., unknown) threats or hazards? Note: Threat/hazard assessments are often included as part of a wider risk assessment?	No



Category	Best Practice	Score
Category 1: Risk Assessment	Best Practice 1.1: The DOT conducts rigorous and candid threat / hazard assessments and consults external stakeholders or peers for review.	Repeatable
	Best Practice 1.2: The threat / hazard assessment includes a process for imagining unknown threats or hazards with the potential to impact the DOT negatively.	Partial



Category 1: Risk Assessment	Best Practice 1.1: The DOT conducts rigorous and candid threat / hazard assessments and consults external stakeholders or peers for review.	Repeatable	**To meet this best practice:** *** It is advised that your organization should consult with external stakeholders or peers for assistance with and/or review of its** * *	[Link 1] [Link 2] [Link 3]



SECURITY PARAMETERS

Partial

Security Awareness

Identify processes and integrated programs to centralize security data.

Informed

Security Awareness

Integrate Security

Demonstrate and communicate concepts of deter, detect, delay, and deny in internal processes and programs across operations. Prioritize activities based on objectives, the environment, and requirements.

Repeatable

Security Awareness

Integrate Security

Security Ecosystem

Standardize and enforce security best practices in planning and design. Incorporate iterative reviews to accommodate a dynamic environment.

Adaptive

Security Awareness

Integrate Security

Security Ecosystem

Institutionalize Security

Maintain and grow the capacity to adapt practices based on predictive factors impacting the internal and external security ecosystem.

Exceeds Threshold

Exceeds Threshold is a parameter that dynamically reinforces ongoing adaptive practices.

Parameter Guidelines

Guidelines indicate increasing levels of security capacities, building upon the previous level.

Poll – Which Security Parameter does your organization identify with best?

- **Security Awareness** – Identify processes and integrate programs to centralize security data.
- **Integrate Security** – Demonstrate and communicate concepts to deter, detect, delay, and deny in internal processes and programs across operations.
- **Security Ecosystem** – Standardize and enforce security best practices in planning and design.
- **Institutionalize Security** – Maintain and grow the capacity to adapt practices based on predictive factors impacting the security ecosystem.
- **Exceeds Threshold** – Dynamic reinforcement of ongoing adaptive practices.

Advancing Security Parameters

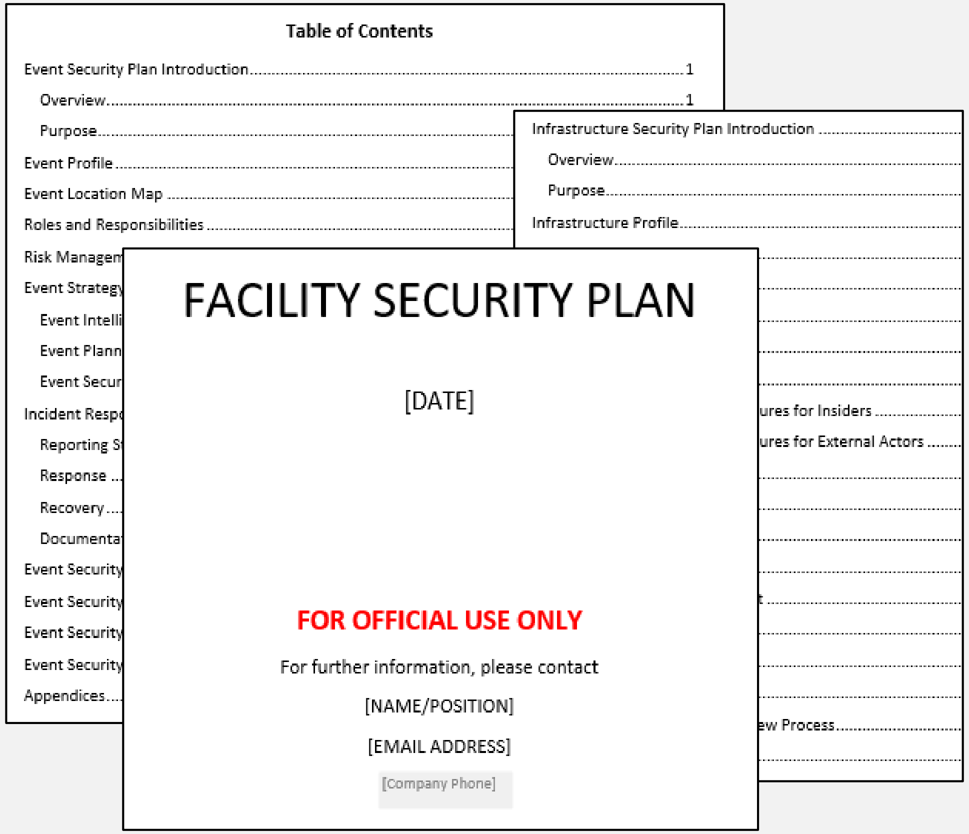


Table of Contents

FACILITY SECURITY PLAN

[DATE]

FOR OFFICIAL USE ONLY

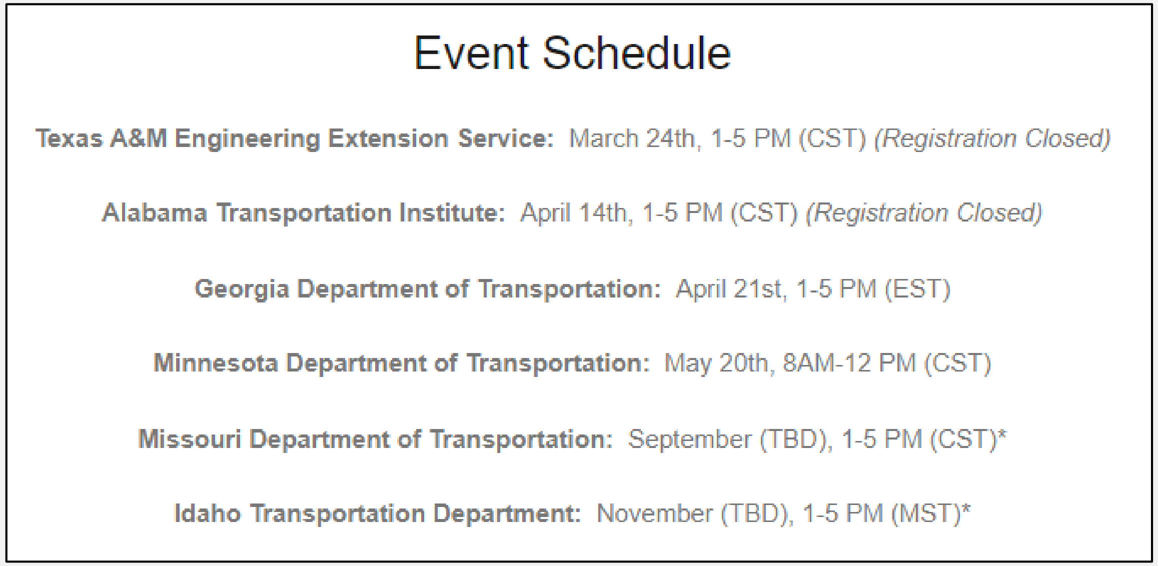
For further information, please contact

[NAME/POSITION]

[EMAIL ADDRESS]

[Company Phone]

Source: https://www.achrnews.com/articles/140507-online-opportunities-all-the-benefits-of-hvac-training-without-the-expense-of-travel



Event Schedule

Texas A&M Engineering Extension Service: March 24th, 1-5 PM (CST) *(Registration Closed)*

Alabama Transportation Institute: April 14th, 1-5 PM (CST) *(Registration Closed)*

Georgia Department of Transportation: April 21st, 1-5 PM (EST)

Minnesota Department of Transportation: May 20th, 8AM-12 PM (CST)

Missouri Department of Transportation: September (TBD), 1-5 PM (CST)*

Idaho Transportation Department: November (TBD), 1-5 PM (MST)*

Registration: https://criticalops.com/trbevents/

National Workshop and Training Class

- Emergent Security Concepts training class open to all interested in the topic.
- Curriculum is based on universal security best practices and fulfills learning objectives mapped to security research catered to the State Departments of Transportation (DOT).
- Consists of a mixture of training and interactive content, along with supporting materials and guidance.
  - Terms and Definitions: Establish a Common Language
  - Industry Examples
  - “Event-Based” Security Exercise

Curriculum Overview

- **Module 1**: Infrastructure Security
  - Physical Infrastructure Security, Cybersecurity, Convergence, Resilience, All-Hazards Emergency Preparedness, Continuity Of Operations
- **Module 2**: Personnel Security
  - Security Training and Education, Insider Threat, Workplace Violence, Operational Security, Social Media Training
- **Module 3**: Physical Security
  - Threat, Vulnerability and Risk Assessments, Layered Defense, Deterrence, Access Control, Bomb Threat Response, Hardening Tactics, Realistic and Effective Exercises
- **Module 4**: Security Management
  - Security Planning and Budgeting, Crisis Response, Crisis Communication, Security Incident Discovery, Response and Investigation, Change Management Strategies

Summary

- Security Awareness
- Customized Integration
- Enforceable Security Standards
- Dynamic Knowledge Acquisition

Contact Information

- Chelsea Treboniak, chelsea@criticalops.com, (443) 404-1879
- Jenni Hesterman, jennihesterman@gmail.com, (571) 289-7225
- Stephen Terhaar, stephen.Terhaar@state.mn.us, (651) 717-5924
- Neal “Murph” Murphy, neal.murphy@itd.Idaho.gov, (208) 334-8414

Today's Panelists

#TRBWebinar

Moderator: Chelsea Treboniak

CRITICAL OPS LLC

Stephen Terhaar

mn DEPARTMENT OF TRANSPORTATION

Neal Murphy

IDAHO TRANSPORTATION DEPARTMENT

Jenni Hesterman, *Independent Consultant*

TRB’s New Podcast!

- Have you heard that we have a new podcast, TRB’s Transportation Explorers?
- Listen on our website or subscribe wherever you listen to podcasts!

#TRBExplorers

Get Involved with TRB

Receive emails about upcoming TRB webinars
https://bit.ly/TRBemails

#TRBwebinar

Find upcoming conferences
http://www.trb.org/Calendar

@NASEMTRB

@NASEMTRB

Transportation Research Board

Get Involved with TRB

#TRBwebinar

@NASEMTRB

@NASEMTRB

Transportation Research Board

Getting involved is free!

Be a Friend of a Committee bit.ly/TRBcommittees

– Networking opportunities

– May provide a path to Standing Committee membership

Join a Standing Committee bit.ly/TRBstandingcommittee

Work with CRP https://bit.ly/TRB-crp

Update your information www.mytrb.org