The Future of Cybersecurity – Cyber Resiliency Workshop Motor Freight Traffic - Critical Infrastructure

Facilitators:

Michael Wickham, Johns Hopkins University Applied Physics Lab, michael.wickham@jhuapl.edu

John Talieri, National Motor Freight Trade Association, John.Talieri@nmfta.org

NMFTA

National Motor Freight Traffic Association, Inc.

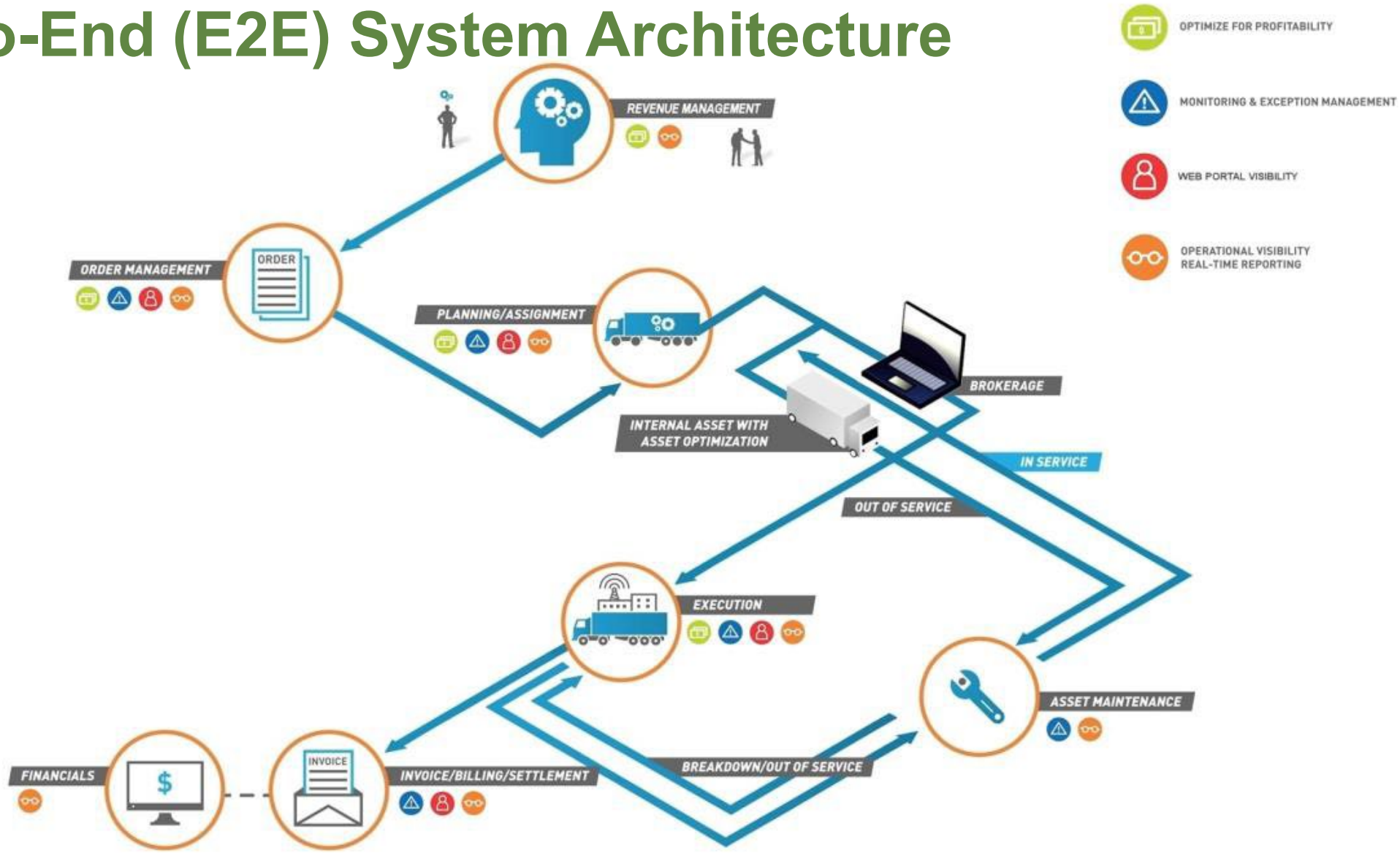
Workshop Agenda

- Applied Workshop (2 hours)– Outcomes – Procedures – working groups
- Cybersecurity Resiliency – definition, assumptions and application, Risk Management and Threat(s), Cybersecurity Managed Service Providers (MSP) companies
- Cybersecurity Standards, Framework, and Best Practices - Guest Presenter Gary Stoneburner, JHU APL
- Managed Service Provider/ Incident Response Guest Presenter – Art Ocain, Airiam

Agenda Continued

- Review and refine Motor Freight Transportation Architecture (MFTA) for Cyber Resilience Analysis
- Define Mission Critical systems and High value targets in the MFTA for your stakeholders
- Attack Incident Case Study – A carrier dispatch systems is attacked with ransomware
- Future – DHS CISA CRR self analysis group exercise
- Future – Cyber Table Top Exercise(s) (CTTX) – DHS CISA CTTX Guidance
- Discussion of What, How, and When can NMFTA assist your stakeholders with Cybersecurity/resiliency/ and survivability?
- Question and Answer session
- Backup slides – MITRE CREF Navigator – Collection of tools

End-to-End (E2E) System Architecture



Cybersecurity Standards, Framework, and Best Practices

Guest Presenter - Gary Stoneburner

Johns Hopkins University Applied Physics Lab

NMFTA

National Motor Freight Traffic Association, Inc.

Cybersecurity Managed Service Provider (MSP) and Incident Response (IR)

Guest Presenter – Art Ocain

Airaim

NMFTA

National Motor Freight Traffic Association, Inc.

End–to-End (E2E) Architecture Working Session "Your Survey Priorities"

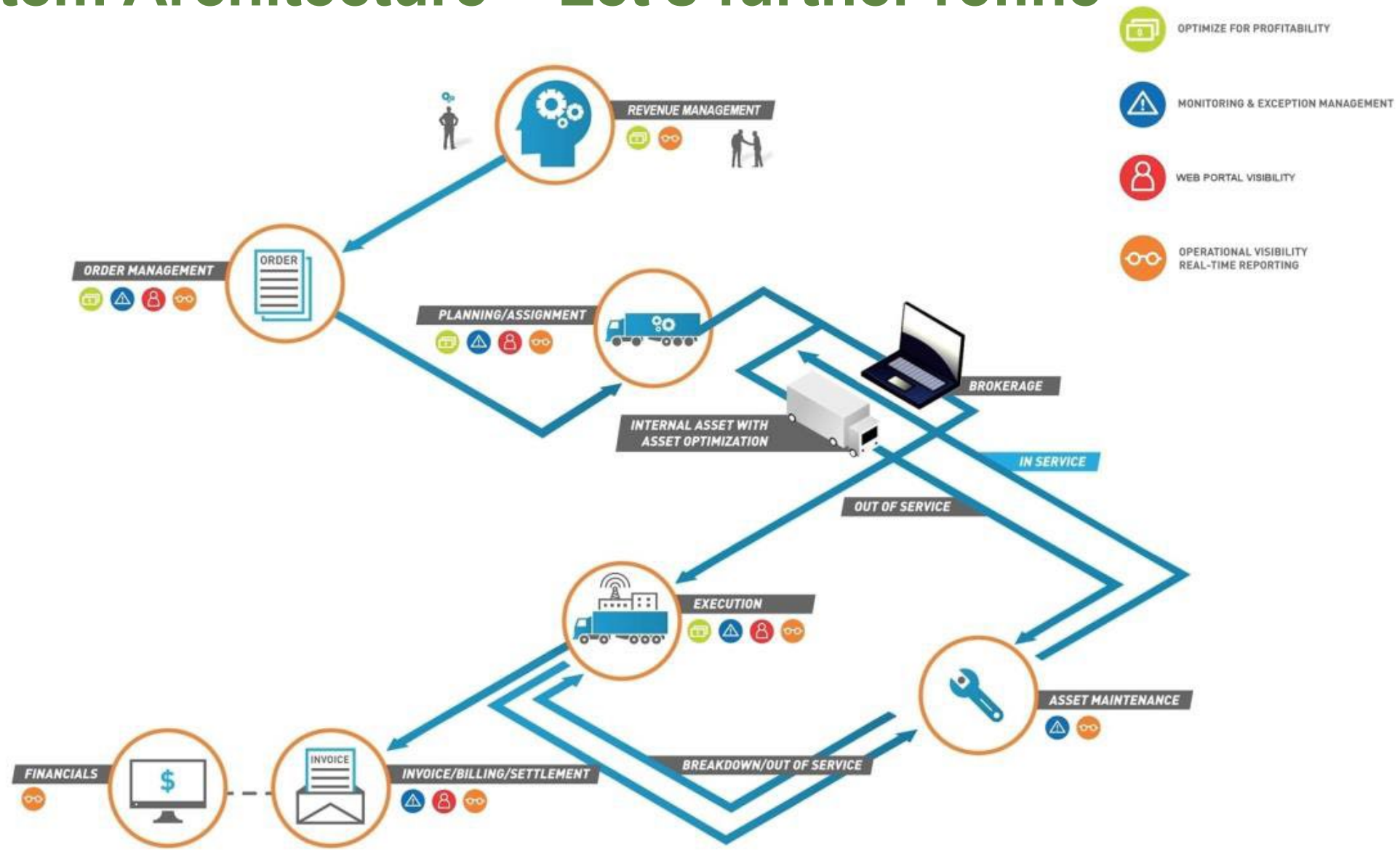
As a group Let's

1) Refine Heavy Vehicle Trucking E2E architecture – Artifact for Analysis
2) Define the stakeholder's Mission Critical systems and High Value Assets – "What to Protect for Mission Assurance"
3) Analyze a hypothetical cyber attack use case and look at system resiliency and survivability during the attack and recovery

NMFTA

National Motor Freight Traffic Association, Inc.

E2E System Architecture – Let's further refine



NMFTA
National Motor Freight Traffic Association, Inc.

Incident Response to Cyber Attack Accomplish your Mission Through the Attack “Mission Assurance”

Let’s Talk Operator talk not Cyber Geek

Know what the Operator needs accomplished

NMFTA

National Motor Freight Traffic Association, Inc.

Survey Results

- Training and Education – 10 votes
- Vehicle Cybersecurity – 6 votes
- Building in security by design versus adding it as an afterthought – (Cybersecurity Requirements) - 3 votes
- Security Operations Center (SOC) solutions and services – 2 votes
- Shift from on premise to cloud security – 1 vote
- Cybersecurity for Heavy Vehicle Electrification and Charging Infrastructure – 0 votes
- End to End Security (from customer to office to truck) – 0 votes
- Enterprise Security – negative 1 vote

Accomplish your Mission Through the Attack "Mission Assurance" - Cyber Resiliency – Applied Workshop

- Identify Critical Mission Areas based on survey - You decide the content of the workshop - Break off into groups
- Refine your Mission area and document on E2E Architecture
- Identify the Mission Critical Systems "Protect the Crown Jewels"
- Identify what Mission Assurance means for your system – What is minimal reduced system that will allow Mission Assurance
- Define ways or controls to accomplish Mission Assurance during the Cyber incident
- Identify recovery strategies

CISA

CYBER RESILIENCE REVIEW (CRR)

“ Mission Assurance Groups” - Cyber Resiliency Applied Workshop

1. \
2. \
3. \
4. \
5. \
6. \
7. \
8. \

Future Cybersecurity Readiness Review (CRR) self analysis group exercise

US Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA) Cybersecurity Readiness Review (CRR)

NMFTA

National Motor Freight Traffic Association, Inc.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Cybersecurity Readiness Review (CRR)

- The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices.
- The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals.
- The CRR assesses enterprise programs and practices across a range of ten domains including risk management, incident management, service continuity, and others.
- The assessment is designed to measure existing organizational resilience as well as provide a gap analysis for improvement based on recognized best practices.

https://www.cisa.gov/uscert/sites/default/files/c3vp/csc-crr-self-assessment-package.pdf

CISA CRR Relationship to the Cybersecurity Framework

- While the CRR predates the establishment of the Cybersecurity Framework, the inherent principles and recommended practices within the CRR align closely with the central tenets of the Cybersecurity Framework.
- The CRR enables an organization to assess its capabilities relative to the Cybersecurity Framework and a crosswalk document that maps the CRR to the NIST Framework is included as a component of the CRR Self-Assessment Package.
- Though the CRR can be used to assess an organization's capabilities, the Framework is based on a different underlying framework and as a result an organization's self-assessment of CRR practices and capabilities may fall short of or exceed corresponding practices and capabilities in the Framework.
- A mapping of the CRR to the Cybersecurity Framework is available here: CRR NIST Framework Crosswalk.

https://www.cisa.gov/uscert/sites/default/files/c3vp/csc-crr-nist-framework-crosswalk.pdf

Cybersecurity Framework - Ten Domains

CYBER RESILIENCE REVIEW (CRR)

NIST Cybersecurity Framework Crosswalks

- One of the foundational principles of the CRR is that an organization deploys its assets (people, information, technology, and facilities) in support of specific operational missions or critical services.
- Applying this principle, the CRR seeks to understand an organization's capabilities in performing, planning, managing, measuring, and defining operational resilience practices and behaviors through an examination of the following ten domains.

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependency Management
9. Training and Awareness
10. Situational Awareness

https://www.cisa.gov/uscert/sites/default/files/c3vp/csc-crr-nist-framework-crosswalk.pdf

Future Endeavors
DHS CISA CRR 6-8 hour Working Group conducted by DHS CISA

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

https://www.cisa.gov/uscert/resources/assessments

NMFTA

National Motor Freight Traffic Association, Inc.

Future – Cyber Tabletop Exercise(s) (CTTX) – using DHS CISA Tabletop Exercise Package (CTEP)

CISA Tabletop Exercise Package

Exercise Planner Handbook

https://www.cisa.gov/cisa-tabletop-exercise-packages

NMFTA

National Motor Freight Traffic Association, Inc.

DHS CISA Tabletop Exercise Package (CTEP)

- **ISA Tabletop Exercise Packages (CTEPs)** are a comprehensive set of resources designed to assist stakeholders in conducting their own exercises. Partners can use CTEPs to initiate discussions within their organizations about their ability to address a variety of threat scenarios.
- Each package is customizable and includes template exercise objectives, scenarios, and discussion questions as well as a collection of references and resources.
- Available scenarios cover a broad array of physical security and cybersecurity topics, such as natural disasters, pandemics, civil disturbances, industrial control systems, election security, ransomware, vehicle ramming, insider threats, active assailants, and unmanned aerial systems. CTEPs also provide scenario and module questions to discuss pre-incident information and intelligence sharing, incident response, and post-incident recovery.

With over 100 CTEPs available, stakeholders can easily find resources to meet their specific exercise needs.

https://www.cisa.gov/cisa-tabletop-exercise-packages

What, How, and When can NMFTA assist your stakeholders with Cybersecurity/resiliency/ and survivability?

NMFTA

National Motor Freight Traffic Association, Inc.

Q & A

NMFTA

National Motor Freight
Traffic Association, Inc.

Backup Slides

NMFTA

National Motor Freight
Traffic Association, Inc.

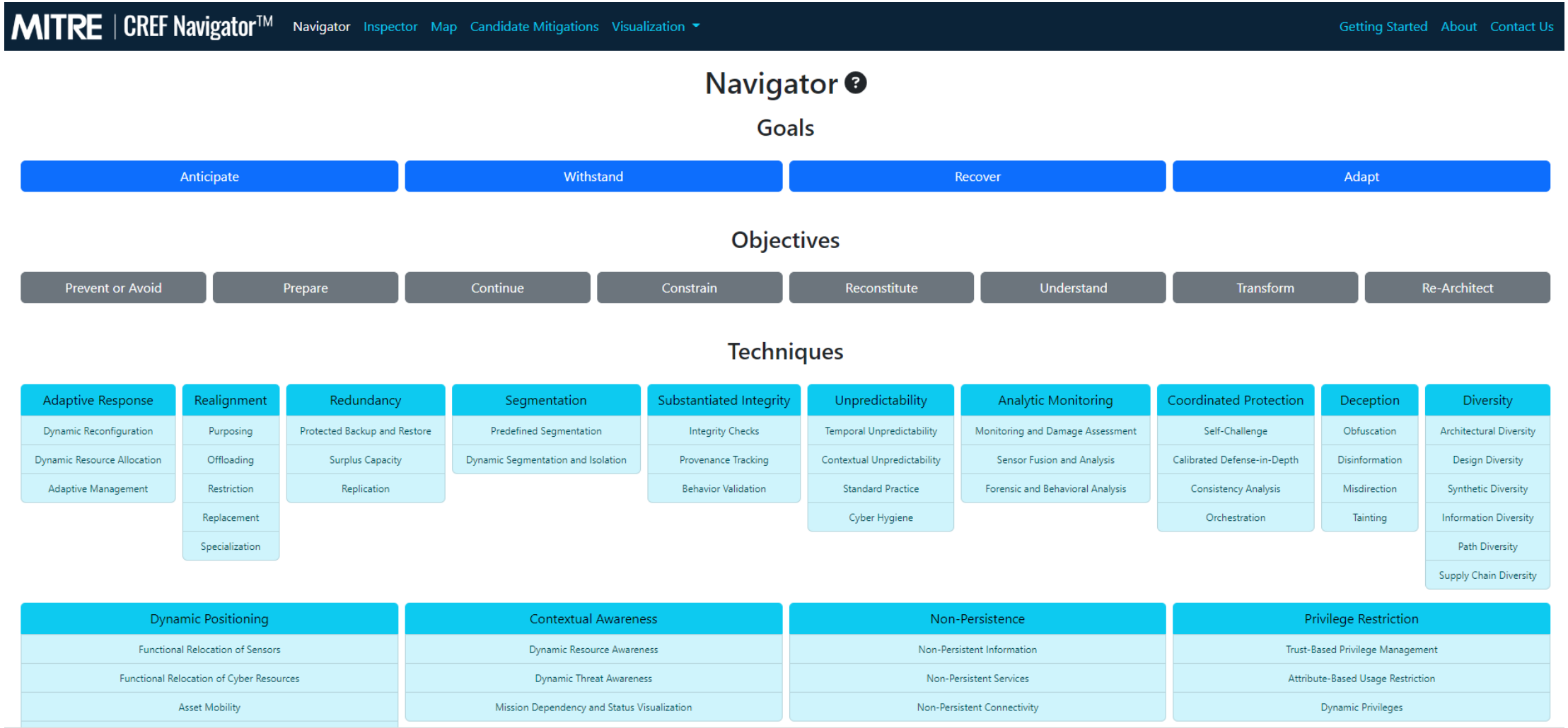
MITRE Cyber Resiliency Engineering Framework (CREF)

CREF Navigator Purpose

- Cyber Resiliency Engineering Framework (CREF) is a MITRE developed cyber security framework that has been incorporated into NIST SP 800-160 Volume 2 (rev 1).
- The CREF Navigator was developed to create a platform in which the complex relationships of NIST SP 800-160 Volume 2 can be searched and visualized, enabling engineers to educate & inform choices while designing resilient cyber solutions.
- The Result: a relational database of NIST SP 800-160 Volume 2 concepts that is searchable, visualizes resilience relationships & presents a Web UI while utilizing portable, opensource components to enable use in tools. The CREF Navigator distills tons of useful terms, tables, and relationships from the CREF/NIST SP 800-160 Volume 2 into an online tool.

https://crefnavigator.mitre.org/navigator

MITRE Cyber Resiliency Engineering Framework (CREF)



https://cretnavigator.mitre.org/navigator

NMFTA National Motor Freight Traffic Association, Inc.

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

A Short History of the NIST Risk Management Framework (RMF)

Gary Stoneburner
Gary.Stoneburner@jhuapl.edu

NIST Special Publications 800 series

NIST
INFORMATION TECHNOLOGY LABORATORY

- NIST Special Pub SP-800-160 volume 2 rev 1 “Cyber Resiliency Engineering Framework” (CREF)
- SP 800-53 “Security and Privacy Controls”
- SP-800-37 “Risk Management Framework for Information Systems and Organizations”
- As it pertains to Motor freight transportation system

https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information

www.nmfta.org