

# RSA® Conference 2022

San Francisco & Digital | June 6 – 9

## TRANSFORM

SESSION ID: SAT-W01

# Protecting Against Evolving Threats to the Global Shipping Infrastructure

**Suzanne Lemieux**

American Petroleum Institute  
Director, Operations, Security  
& Emergence Response Policy

**Alan Dinerman**

The MITRE Corporation  
Advancing Technologies,  
Department Manager

**Josephine Long**

1898 & Co.  
Senior Industrial  
Cybersecurity Program Manager



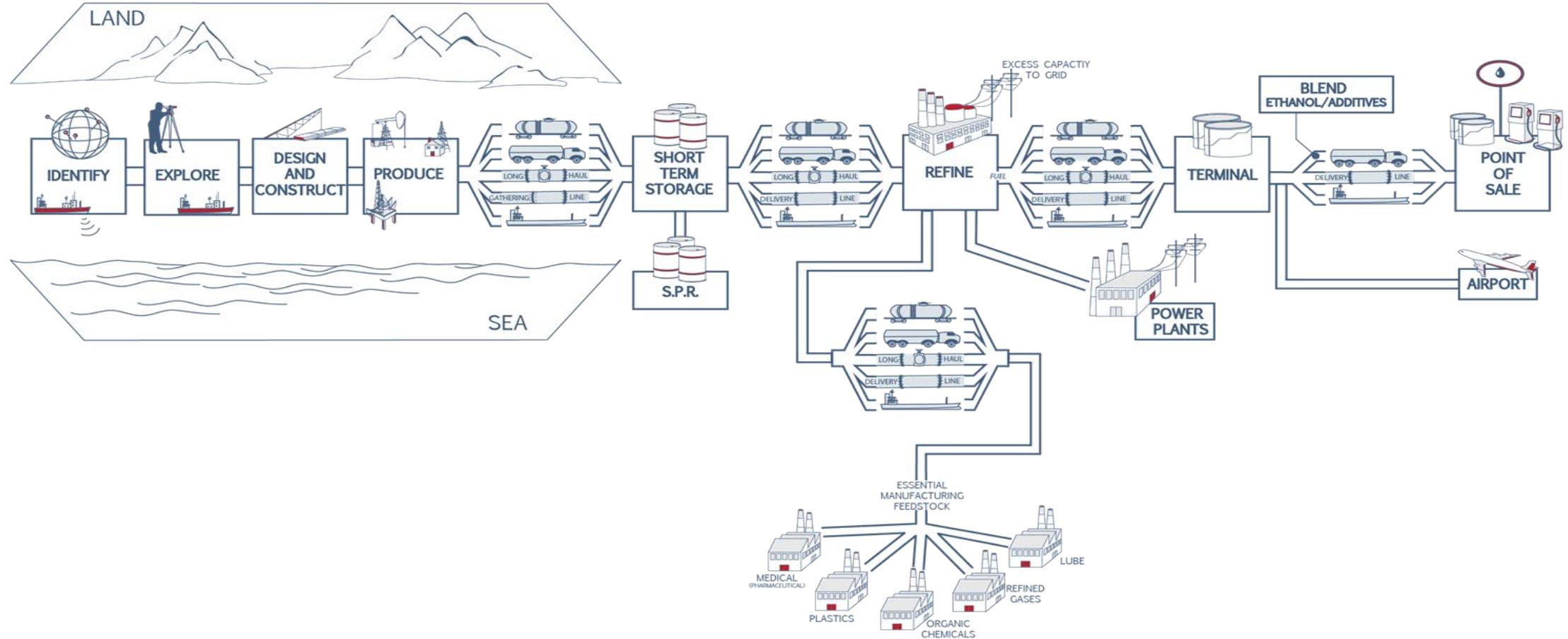
# Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA® Conference, RSA Security LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Security LLC or its affiliates. All rights reserved. RSA Conference logo, RSA and other trademarks are trademarks of RSA Security LLC or its affiliates.

# The global liquids supply chain



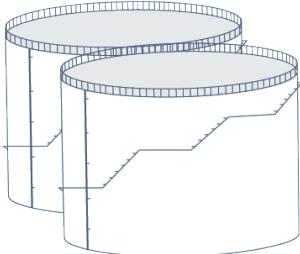
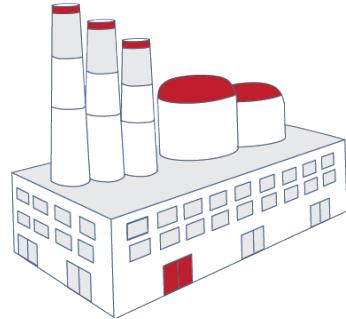
# Critical Components of the System



PRODUCTION



PIPELINES

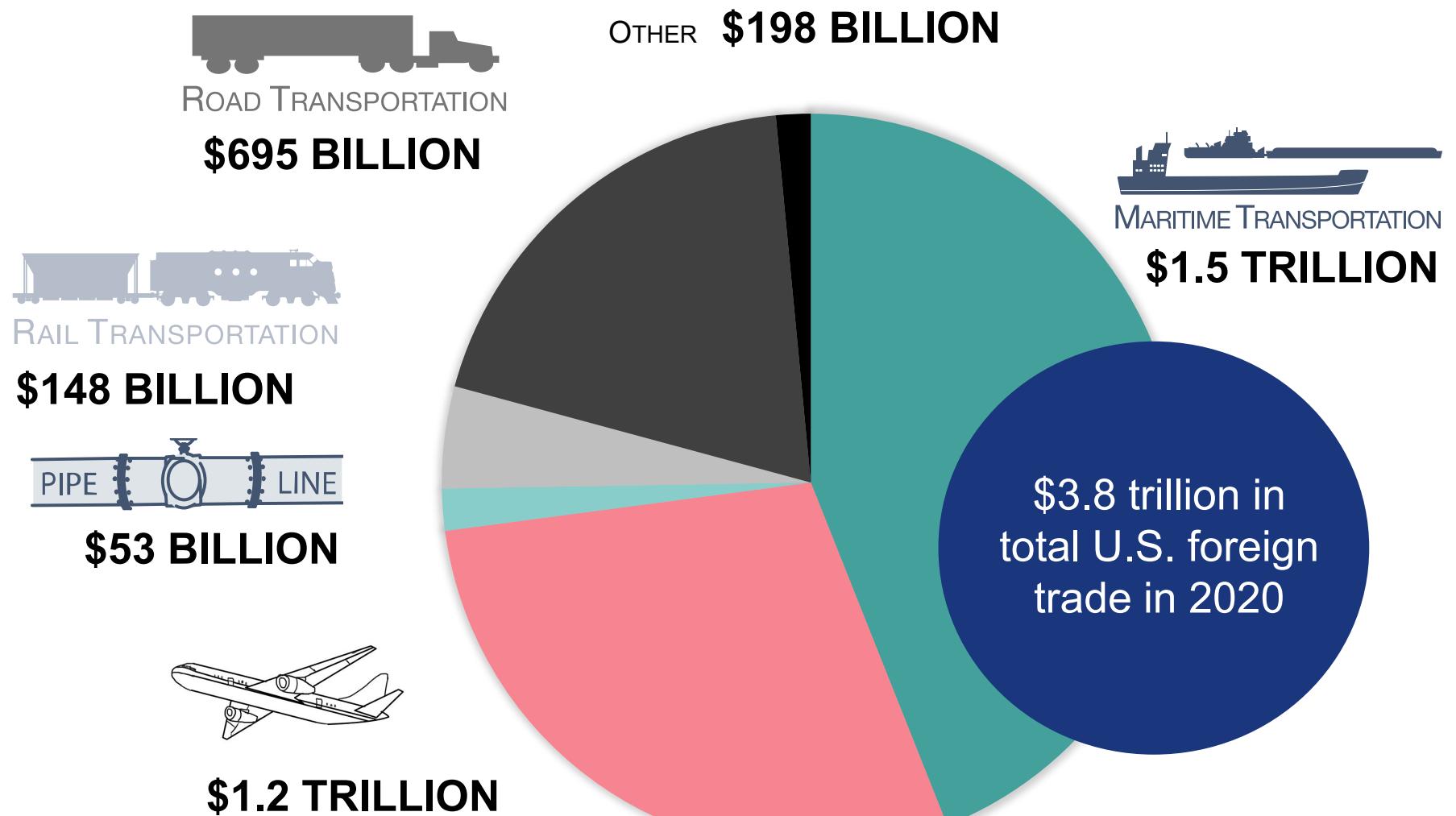
SHORT TERM  
STORAGESHIPPING & PORTS  
OF CALL

REFINING

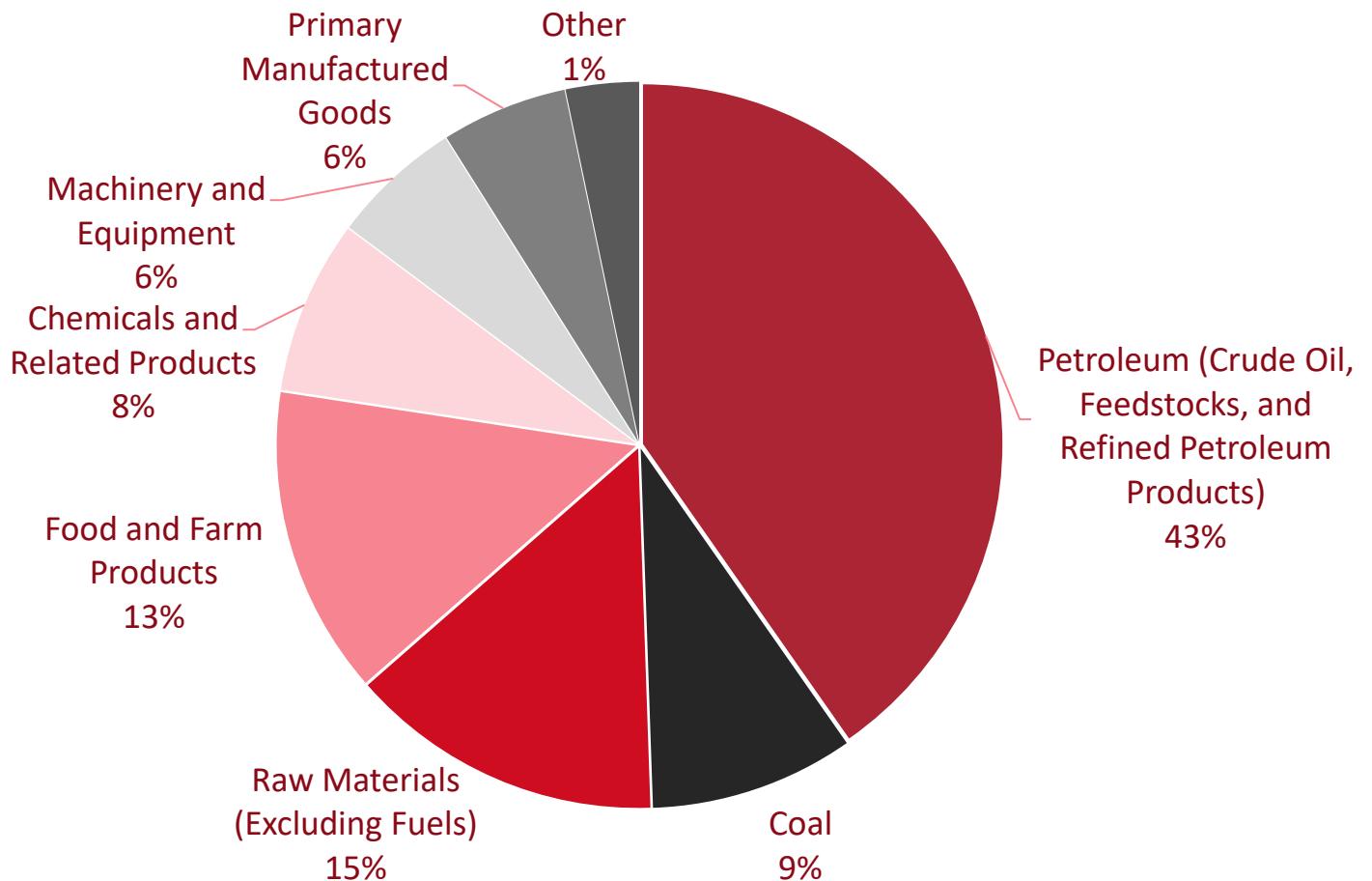


POINT OF SALE

# Foreign Trade on US Infrastructure



# Importance of the MTS to Energy



**SHORT TONS TRANSPORTED VIA WATER IN 2017  
BY COMMODITY GROUP**



U.S. DEPARTMENT OF  
**ENERGY**

American  
Petroleum  
Institute

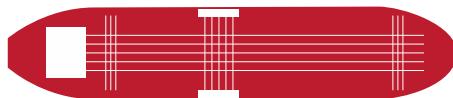
OFFICE OF  
Cybersecurity, Energy Security  
and Emergency Response



1898&Co  
PART OF BURNS & MCDONNELL

RSA Conference 2022

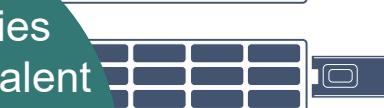
# How the MTS Supports Safety & Efficiency



**One Tanker =**

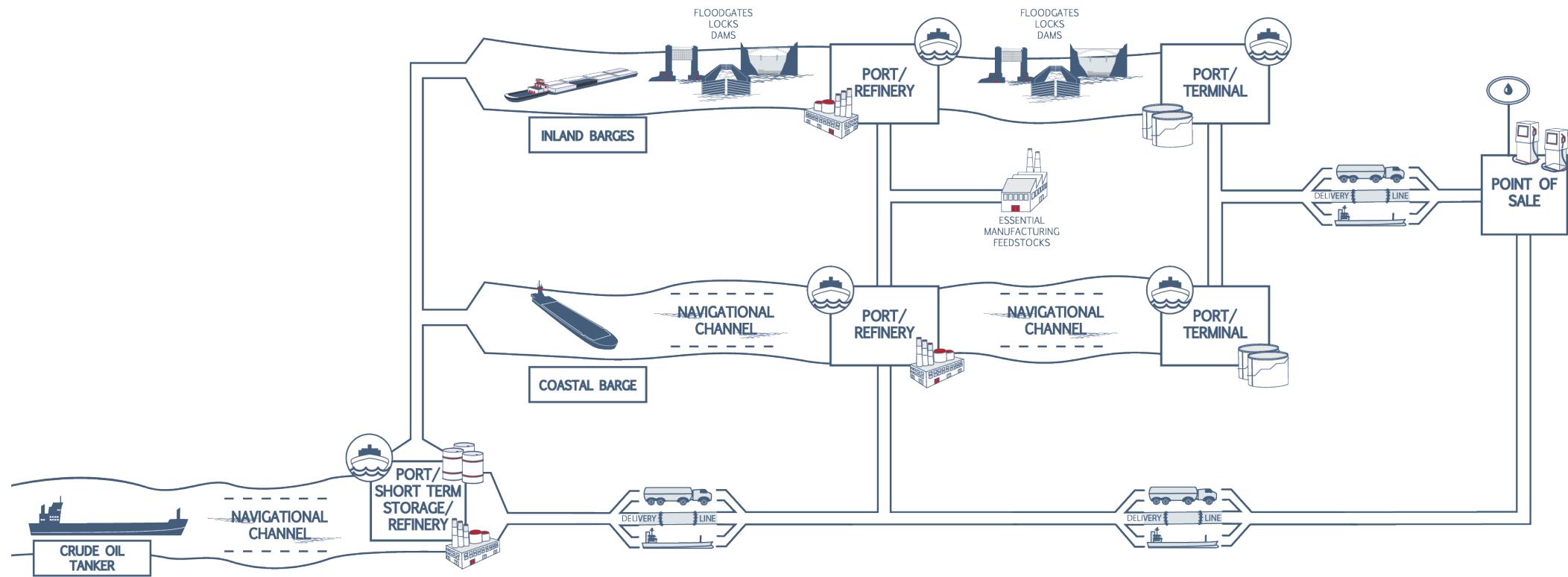


One tanker carries the tonnage equivalent to several common inland barge tows or thousands of rail cars or trucks.



Waterways are the most efficient way of transporting everyday products – from petroleum, grain, coal, and farm products to steel, sand, chemicals, and other building supplies – across the country.

# The Elements of the MTS & the Energy System



Maersk CEO “In the last week of the quarter we were hit by a cyber-attack, which mainly impacted Maersk Line, APM Terminals and Damco. Business volumes were negatively affected for a couple of weeks in July and as a consequence, our Q3 results will be impacted. We expect the cyber-attack will impact results negatively by USD 200-300m.”



## Cyber attack update

June 28, 2017

ANNOUNCEMENT

A.P. Møller - Mærsk A/S — cyber attack update

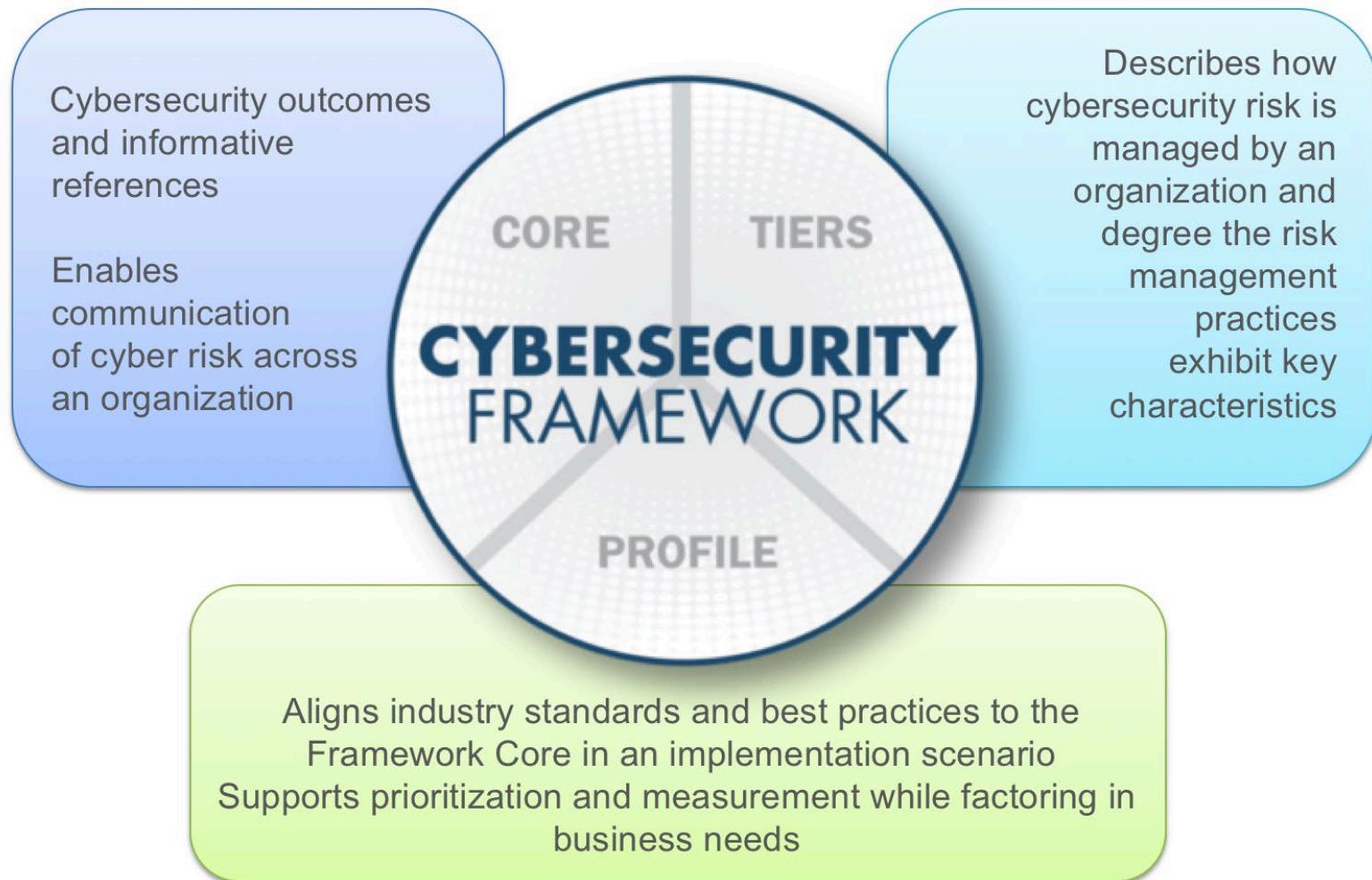
We can confirm that Maersk has been hit as part of a global cyber attack named Petya on the 27 June 2017. IT systems are down across multi and select business units.

RSA® Conference 2022

# NIST Cybersecurity Framework



# NIST Cybersecurity Framework Components



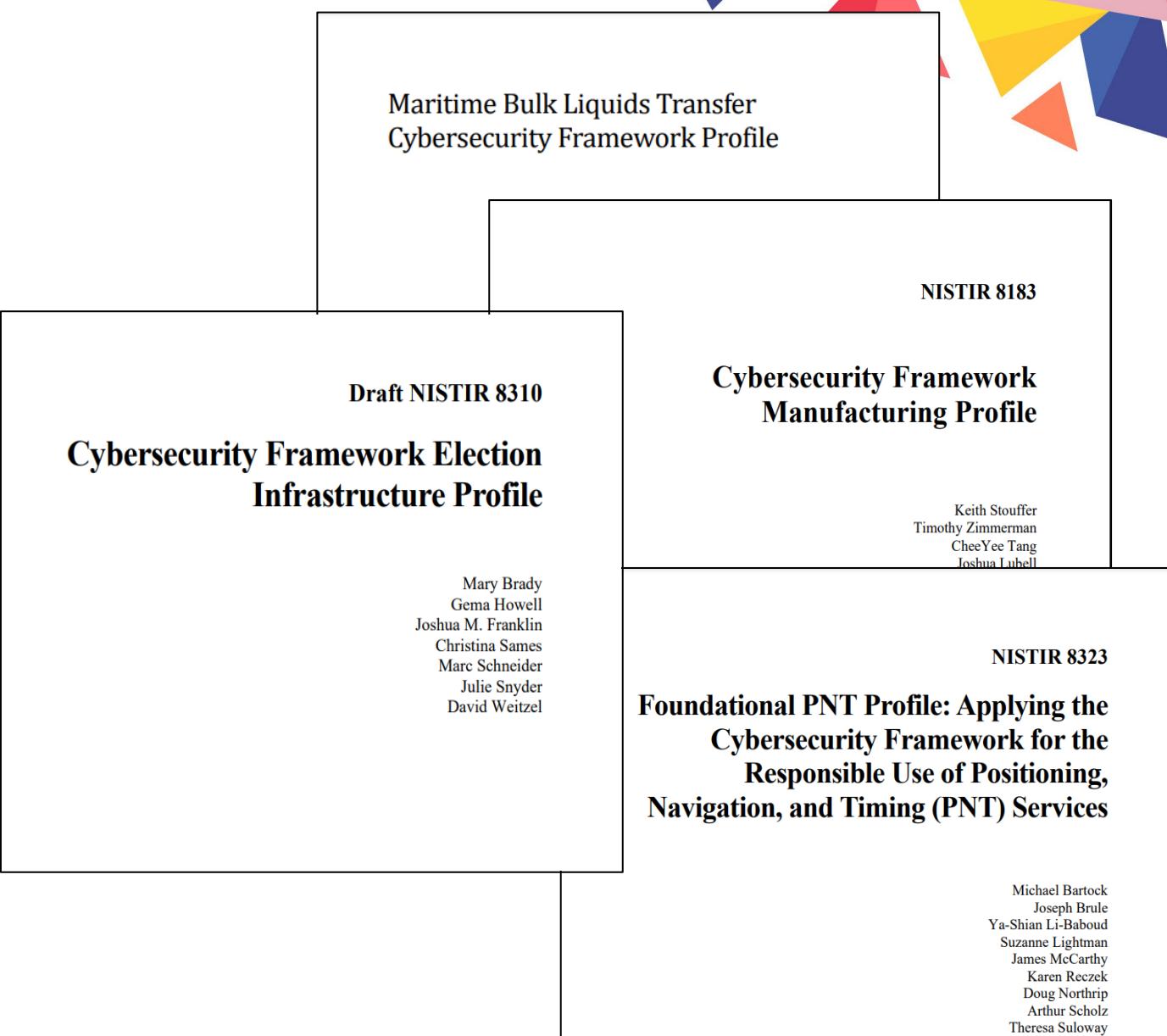
# Framework Functions

- Identify  
What processes and assets need protection?
- Protect  
What safeguards are available?
- Detect  
What techniques can identify incidents?
- Respond  
What techniques can contain impacts of incidents?
- Recover  
What techniques can restore capabilities?



# Profiles built, being built, and to be built

- The Rich History of NIST CSF Profile Building
  - Maritime Bulk Liquid
  - Offshore Operations
  - Passenger Vessel
  - Manufacturing Profile
  - Position, Navigation and Timing
  - Election Systems/Voter Registration
  - Connected Vehicles
  - **Marine Transportation System LNG**
  - Intelligent Transportation (coming soon)



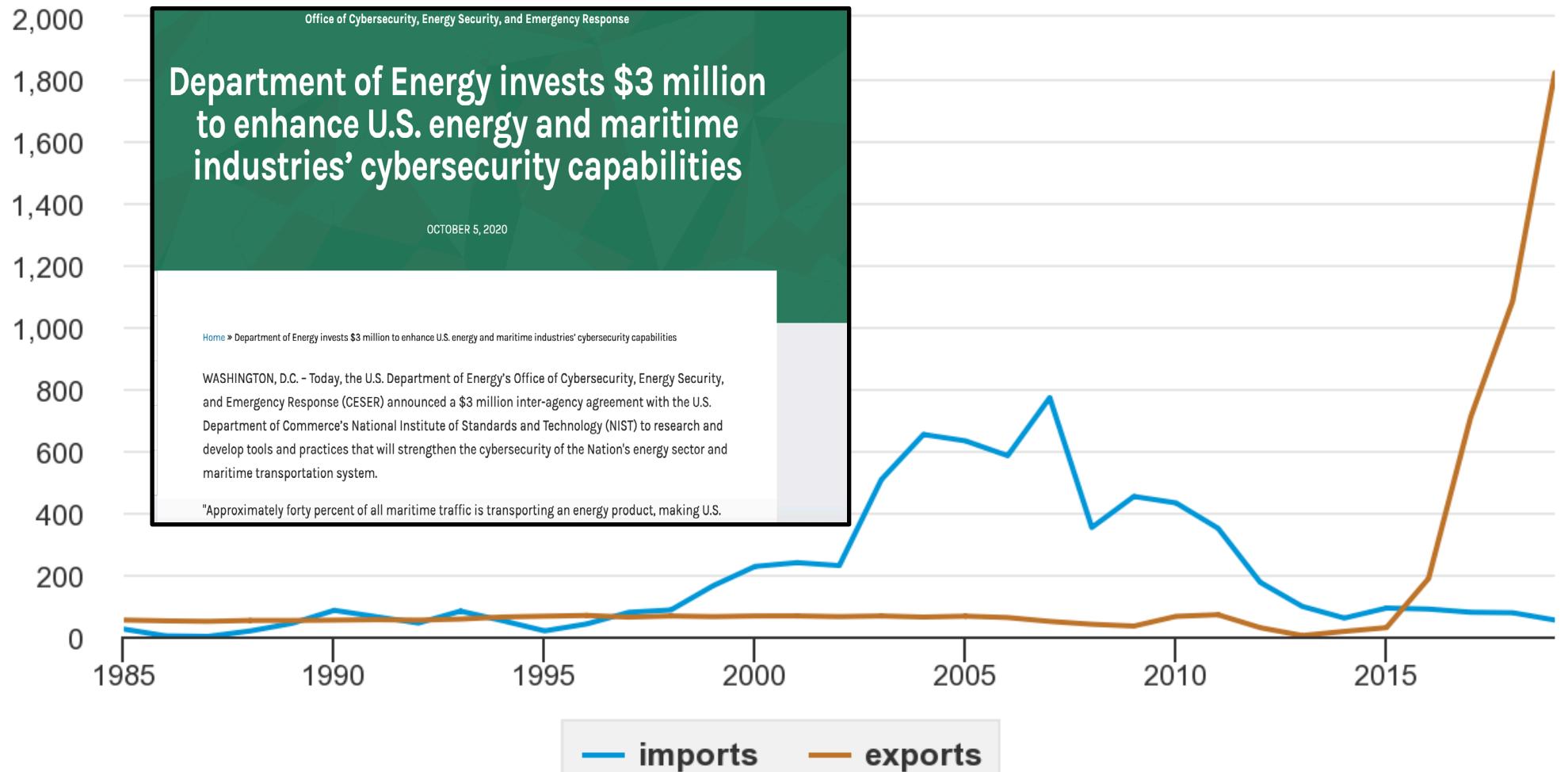
RSA® Conference 2022

# NIST Liquified Natural Gas Cybersecurity Framework Profile



# U.S. LNG imports and exports, 1985-2019

billion cubic feet



Source: U.S. Energy Information Administration, *Natural Gas Monthly*, June 2020

## DOE CESER Project

### Goals:

- Cybersecurity Framework Profile focused on Liquified Natural Gas within the Marine Transportation System
- Enhance Cybersecurity Risk Mitigation Guidance including updating mappings of DOE's Cybersecurity Capability Maturity Model (v2.0) to the Cybersecurity Framework (v1.1)



OFFICE OF  
Cybersecurity, Energy Security  
and Emergency Response



RSA Conference 2022

# Liquified Natural Gas (LNG)

Oil and Natural Gas make up 55 percent of global energy use today. The U.S. Liquid Natural Gas (LNG) industry has grown dramatically in recent years. The American Petroleum Institute projects LNG exports would be a 75-billion-dollar industry to the U.S. GDP by 2035.



**March 2021**

LNG Industry subject matter experts recruited



**April 2021**

Pre-workshop informative cybersecurity framework session



**May 2021**

3 virtual LNG Profile Workshops & Weekly Meetings



## Cybersecurity Framework (CSF) LNG Profile Road Map

**May 2022**

Finalize draft LNG CSF Profile



**Spring 2022**

Profile outreach via posting of Draft LNG CISF Profile (a NISTIR) for public comment

## Why the LNG CSF Profile Is Important

As more crucial technical operations of the LNG lifecycle become fully automated, the need for heightened cybersecurity readiness is necessary to ensure personnel safety, national security interests and environmental safety concerns. This LNG Profile will:

- Inform actions to enhance an organization's cybersecurity posture
- Guide gap analyses of the existing cyber environment
- Support refinement of cybersecurity policies and guidelines



### The CSF Profile

A Cybersecurity Framework Profile is non-regulatory and voluntary guidance that helps identify opportunities for managing cybersecurity risks in a specific industry, trade or organization. The Profile leverages industry-driven expertise to identify Mission Objectives critical to operations and cybersecurity program priorities. The Profile creates a roadmap to align requirements, risk appetite, resources and objectives that are weighed against the Framework Core.



The Profile development team is striving to evolve the use of a CSF Profile to include assessment toolsets, a visual risk dashboard and other dynamic features that will allow organizations to better leverage the efforts of building your custom Profile. Your Profile will be easier to navigate and allow a more expeditious identification of risk control and mitigation procedures.

# NIST CSF LNG Profile

## Categorizing the Mission Objectives Using Theme Buckets

Human Safety	Monitoring Assessment	Plant and Equipment Safety	Corporate Governance	Supply Chain	Quality Control	Regulatory Compliance	Environmental Integrity	Physical Security	Market Share	Trade Secrets
Maintain safe and secure operations	Monitor Detect Respond anomalous behavior	Ensure operational integrity of plant systems & process	Define business policy & governance actions that captures/protects the mission	Validate/ optimize the supply chain	Continually optimize and maintain current operational state by establishing baselines and measures	Maintain regulatory compliance	Safeguard environmental integrity	Maintain & control operational & enterprise security & access		
Maintain personnel safety	Establish baseline/ measure deviation from baseline	Maintain plant systems (Technology)	Measure effective-ness of policies and controls	Secure 3 <sup>rd</sup> Party Supply Chain	Insure efficient port operations	Ensure compliance to applicable standards (ISA 84/IEC61511				
Ensure operational integrity/ Cyber considerations	Manage-ment of alarms	Maintain network monitoring/detection	Maintain containment	Maintain	Maintain					
Identify /measure industry risk	Control Access									
Maintain Protective Functions (SIS)	Sustain/ verify effective-ness of controls									
Maintain separation between the BPCS and Safety Systems	Identify vulnerabilities/ threats									

Rank	Score	Mission Objective	1	2	3	4	5	6
			13	13	13	13	8	13
1	12.2	Maintain safe and secure operations	13	13	13	13	8	13
2*	11.3	Ensure operational integrity of plant systems & process	12	12	0	12	12	0
3*	11.3	Maintain & control operational & enterprise security & access	8	8	8	8	8	8
4	8.8	Safeguard environmental integrity						
5	8.3	Monitor Detect Respond to anomalous behavior						
6	6.2	Define business policy & governance actions that captures/protects the mission						
7	6	Maintain regulatory compliance						
8	4.7	Continually optimize and maintain current operational state by establishing baselines and measures						
9	4.3	Validate/optimize the supply chain						

Function	Category	Subcategory	Mission Objectives							
			●●● = High Priority	●● = Moderate Priority	● = Other Implemented Subcategories					
	Risk Management Strategy (ID.RM):	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	●●●	●●	●	●	●	●	●	●
	ID.RM-1:	Risk management processes are established, managed, and agreed to by organizational stakeholders	●●●	●●	●	●	●	●	●	●
	ID.RM-2:	Organizational risk tolerance is determined and clearly expressed	●●	●●	●	●	●	●	●	●
	ID.RM-3:	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	●●	●●	●●	●●	●●	●●	●●	●●
	PR.AC-1:	Identities and credentials are managed for authorized devices and users	●	●	●●●	●	●	●	●	●●
	PR.AC-2:	Physical access to assets is managed and protected	●	●	●●●	●	●	●	●	●●
	PR.AC-3:	Remote access is managed	●	●	●●	●	●	●	●	●●
	PR.AC-4:	Access permissions are managed, incorporating the principles of least privilege and separation of duties	●	●	●●●	●	●	●	●	●●
	PR.AC-5:	Network integrity is protected, incorporating network segregation where appropriate	●●	●●	●●	●●	●●	●●	●●	●●
	Awareness and Training (PR.AT):	All users are informed and trained	●●●	●●●	●●●	●●●	●●●	●●●	●●●	●●●
	PR.AT-1:	The organization's personnel and partners are	●●●	●●●	●●●	●●●	●●●	●●●	●●●	●●●



U.S. DEPARTMENT OF  
**ENERGY**  
American Petroleum Institute

OFFICE OF  
Cybersecurity, Energy Security  
and Emergency Response



National Institute of  
Standards and Technology  
U.S. Department of Commerce



NCCOE  
NATIONAL CYBERSECURITY  
CENTER OF EXCELLENCE



1898 CO<sup>TM</sup>  
PART OF BURNS & MCDONNELL

RSA Conference 2022

RSA® Conference 2022

# Future of NIST Cybersecurity Framework Profiles

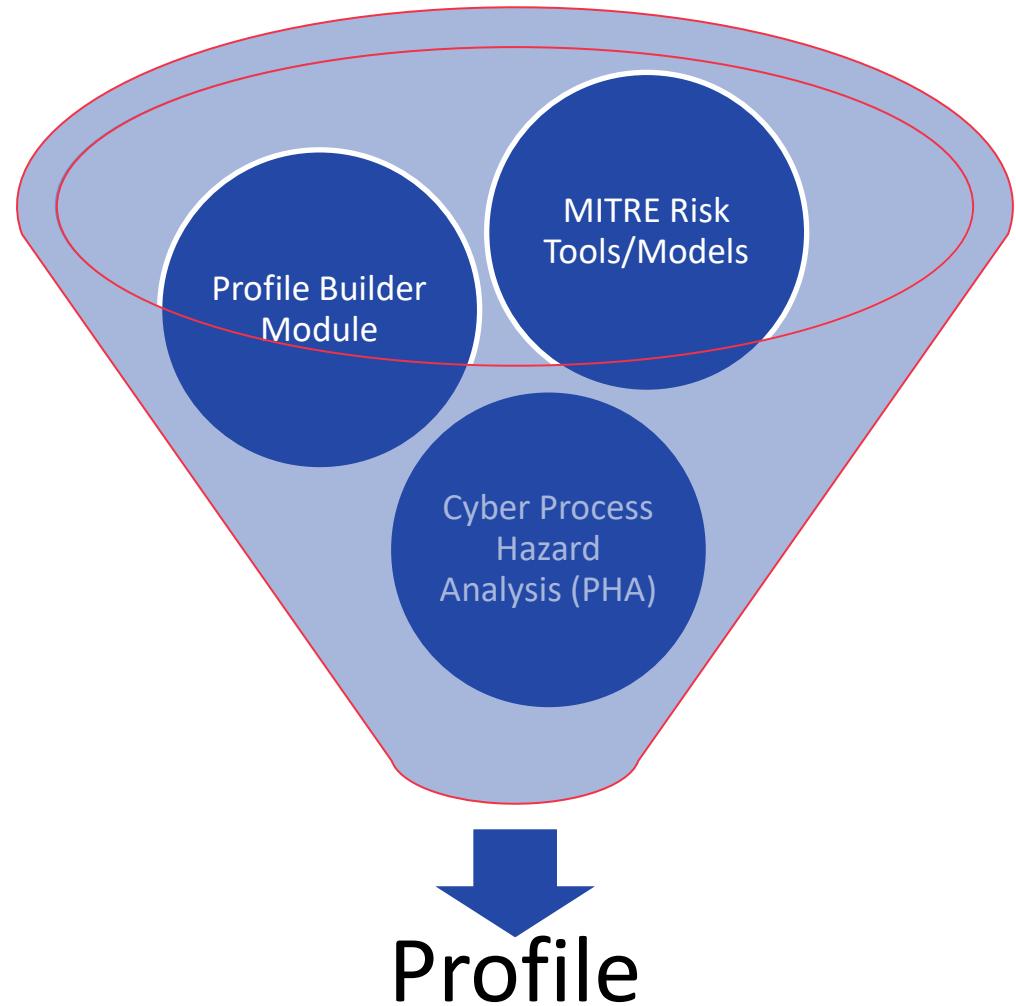


# Evolving to:

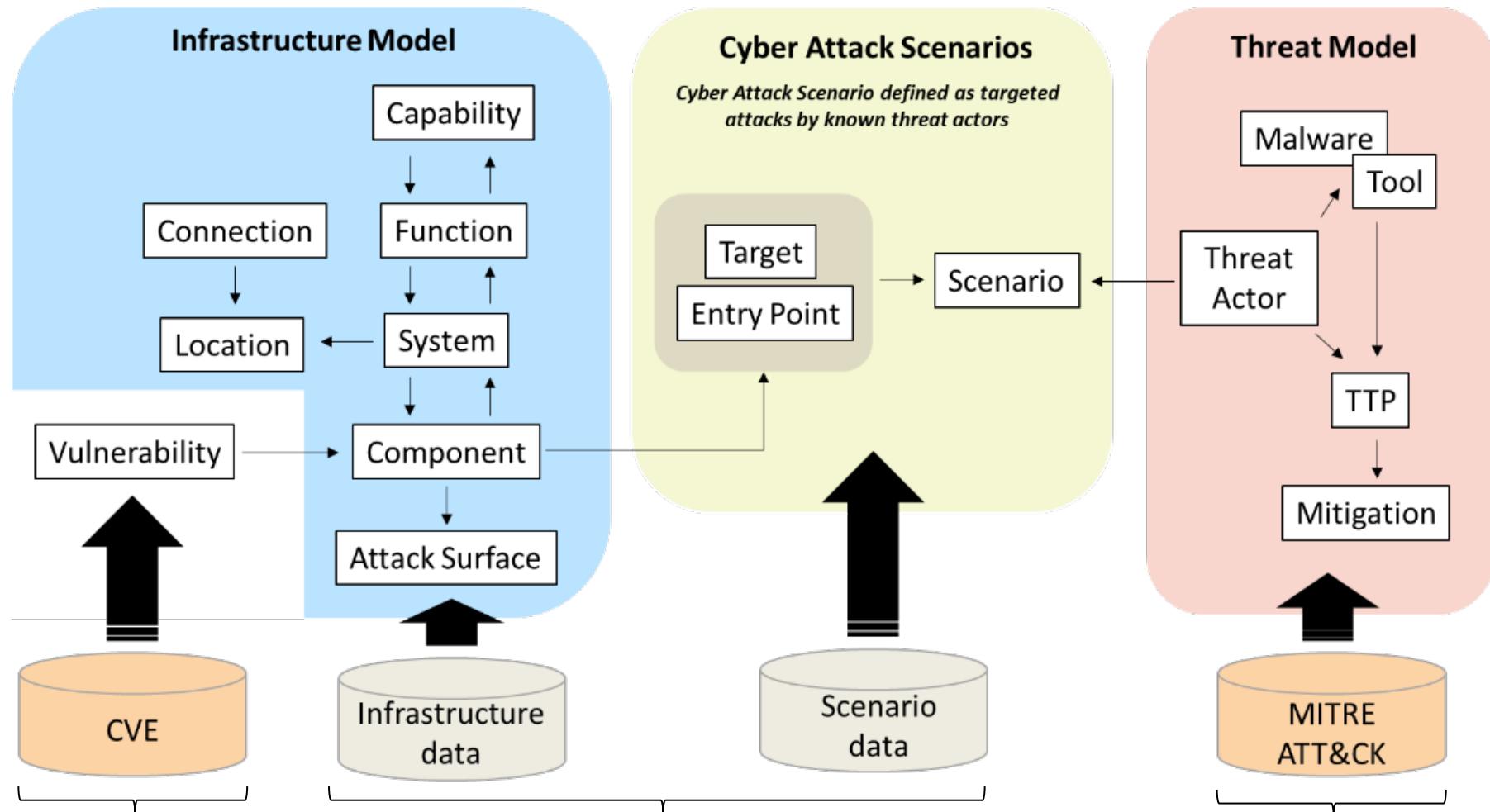


# The Art of the Possible

Use of tools



# MITRE Data Model merges architecture and threat



# What's on the horizon:

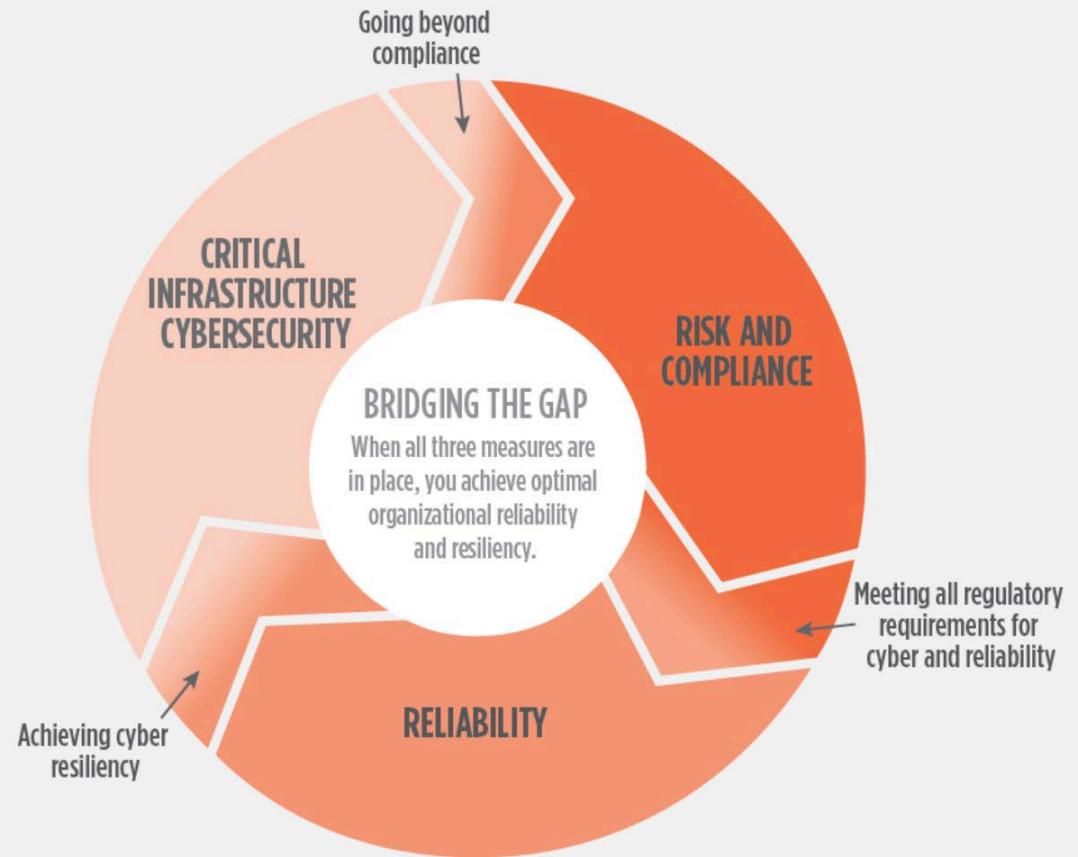
- Pragmatic Process for Implementation
- Gap Analysis Methodology
- Profile Implementation Guide, you have a Profile now what?

RSA® Conference 2022

# Effective Risk Management



# Critical Infrastructure Cybersecurity



# Effective Risk Management



# Apply What You Have Learned Today

- Next week you should:
  - Familiarize yourself with the NIST Cybersecurity Framework.
  - Determine how your organization applies enterprise risk management and relevant guiding doctrine? (consider NISTIR 8286 Integrating Cybersecurity and Enterprise Risk Management (ERM))
  - What is the cybersecurity policy landscape and appetite of your organization?
- In the first three months following this presentation you should:
  - Identify application opportunities of the NIST Cybersecurity Framework, and specifically a CSF Profile.
- Within six months you should:
  - Identify correct organizational players to build a CSF Profile.
  - Create an organizational CSF Profile and establish organization priorities for cybersecurity risk management.

## Additional References:

<https://www.api.org>

[www.nist.gov/cyberframework](http://www.nist.gov/cyberframework)

<https://github.com/mitre/cicat>

<https://attack.mitre.org>

[Microsoft Word - Maritime BLT CSF \(uscg.mil\)](#)

[Homepage | NCCoE \(nist.gov\)](#)

[1898 Home | 1898 & Co. \(burnsmcd.com\)](#)

# For more information please contact:

Suzanne Lemieux at [lemieuxs@api.org](mailto:lemieuxs@api.org)

Alan Dinerman at [adinerman@mitre.org](mailto:adinerman@mitre.org)

Josie Long at [Josephine.long@1898andco.com](mailto:Josephine.long@1898andco.com)