



Mar. 21, 2025

To: International Policy Division, Policy Bureau,  
Ministry of Land, Infrastructure, Transport and Tourism

# A Study on Cybersecurity Related Policies and Current Developments in the U.S. Critical Infrastructure For Public Release / Summary Version

WASHINGTON | CORE



# Structure of the Report

This research project focuses on U.S. cybersecurity policies in infrastructure, ISAC initiatives, domestic production trends, and economic security policies. The findings are compiled into this report, with this section providing a summary of the key points.

## Structure of the Report

### 1 Research on Cyber-attack Cases and Policies in the U.S. Infrastructure Sector

#### Six Sectors



Aviation & Airports



Railroads



Transportation  
(connected cars, etc.)



Port & Transportation  
(Vessels)



Water  
supply



Dams



#### 1) Cyber Security Threats and Examples

Threat  
Landscape

Attack  
Cases

#### 2) Cyber Security Agencies

#### 3) Preparedness for Cyberattacks

Regulations

Funding Programs

Strategies and  
Guidelines

Awareness  
Initiatives

#### Cross-sector Regulations

### 2 U.S. ISAC initiatives in the infrastructure sector

#### 1) Overview of ISACs in the U.S. Infrastructure Sector

#### 2) Overview, activities, and U.S. government collaboration of seven ISACs:

Aviation

Marine  
Transportation

Real  
Estate

Ground  
Transport

Public  
Transportation

Automobile

Water

### 3 Research on U.S. Domestic Production Policies in Infrastructure

#### 1) Trends & policies in U.S. infrastructure domestic production

#### 2) Major federal policy developments

#### 3) WTO rules implications

### 4 Research on Economic Security in U.S. Infrastructure

#### 1) CFIUS regulations on foreign investment for economic security

#### 2) Cybersecurity measures for submarine cables

#### 3) Maritime transportation policies

#### 4) Regulations excluding specific companies

### 5 Future Directions

#### 1) Policy directions for MLIT initiatives

#### 2) Future approach for Japan's ISAC efforts

#### 3) Key considerations and opportunities for Japanese companies in overseas infrastructure expansion

# Aviation and Airports

## Overview of Threats

Airline and airport companies process data on millions of passengers and cargo shipments each year and have access to customer personally identifiable information (PII), payment information, employee data, and biometric authentication.

At the Cybersecurity and Resilience Symposium held in November 2023, the International Civil Aviation Organization (ICAO) warned that cyber attacks on airlines and airports could result in the leakage of passenger data, including names, addresses, and passport numbers, as well as flight cancellations and delays, the impact on connecting flights, the financial consequences, and even catastrophic aircraft accidents and crashes.

Security is also complex due to the variety of systems in airports, including ticketing terminals, baggage self check-in machines, Wi-Fi, parking lot access control systems, and staff authentication systems.

Cybersecurity threats facing the airline and airport industry include ransomware attacks and hacking. In the U.S., cyber threats to the industry are on the rise, and the U.S. had the most cyber attacks targeting the aviation sector in the world, with seven in 2023.

## Relevant Authorities



FAA



TSA



CISA

## Measures & Preparations

### Regulations

- Security Directive on an Emergency Basis
- Advisory Circular (AC): Operational Authorization of Aircraft Network Security Program
- Notice of Proposed Rulemaking: Equipment, Systems, and Network Information Security Protection

### Strategies & Guidelines, etc.

- FAA Cybersecurity Strategy
- Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems (UASs)
- Cybersecurity Guidance: Chinese-Manufactured UAS

### Funding Programs, etc.

- State and Local Cybersecurity Grant Program

### Awareness Campaigns

- Cybersecurity Awareness Symposium
- Be Air Aware™ Program

# Railroad

## Overview of Threats

Rail infrastructure requires robust security measures that provide for the long-term lifecycle of equipment while emphasizing safety. However, many railroad control systems were designed decades ago and often do not have built-in security features, making partial system updates difficult and yet vulnerable due to diverse supply chains and multiple operators with different security practices.

Meanwhile, the increasing integration of critical Operational Technology (OT) and Internet of Things (IoT) solutions is enabling more precise operation schedules and improved operational efficiency. For example, the Positive Train Control (PTC) system, a control system that ensures safe operation, plays an important role in preventing train collisions, over speeding, and derailments due to mis operation. The integration of this PTC system with IoT technology enables real-time data exchange and monitoring of operation status, further improving the safety and efficiency of operation.

Yet, the introduction of these digital technologies has simultaneously brought with it an expansion of cyber threats. In particular, the convergence of IT and OT systems has expanded the attack surface and created new vulnerabilities. Cyber attacks on the rail industry have increased by more than 220% over the past five years, and this trend has a serious impact on the entire industry.

To address these challenges, the railroad industry has adopted a multi-layered defense strategy that includes network segmentation to isolate the affected areas, strict access control, implementation of intrusion detection systems, development of incident response plans, and employee training.

## Relevant Authorities



FTA



FRA



TSA



CISA

## Measures & Preparations

### Regulations

- Security Directive, 1580-21-01A • 1582-21-01A
- Security Directive, 1580-21-01C • 1582-21-01C
- Notice of Proposed Rulemaking: Enhancing Surface Cyber Risk Management

### Strategies & Guidelines, etc.

- Security Risk Management for Connected Railroads
- PTC Communications: Cybersecurity Technology Review and Concept of Operations

### Funding Programs, etc.

- State and Local Cybersecurity Grant Program
- Consolidated Rail Infrastructure and Safety Improvements (CRISI) Program
- Urbanized Area Formula Program

### Awareness Campaigns

- Cybersecurity Awareness for Transit Agencies Webinar



# Transportation (connected cars, etc.)

## Overview of Threats

V2X (Vehicle to X), is a technology that enables communication and coordination between vehicles and various other things (e.g., cars and vehicles, cars and infrastructure equipment around the road) by installing various devices and components in vehicles and connecting them to computer networks at all times. V2X technology has been installed in Cyber threats to connected and self-driving cars are increasing.

With the increase in the number of electric vehicles (EVs), cybersecurity risks in the entire ecosystem of EV power equipment and EV charging infrastructure are also increasing, and attackers may attempt to access user data, interrupt charging, and penetrate networks to disrupt the power grid.

The number of cyberattacks against vehicles reported worldwide has increased since 2017, with 295 in 2023, 95% of which were remote; the most common attack vectors (methods by which attackers penetrate networks and systems) of cyber attacks reported in 2023 were Telematics (a communication system installed in a vehicle to provide various information through two-way reception, such as tracking in case of vehicle theft, location information, and driving history) and cloud computing (43.0%).

## Relevant Authorities



FTA



DOC



CISA



DOE CESER and Joint  
Office of Energy and  
Transportation



## Measures & Preparations

### Regulations

- Final Rule: Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles

### Strategies & Guidelines, etc.

- Cybersecurity Best Practices for Modern Vehicles
- Cybersecurity and Intelligent Transportation Systems – A Best Practice Guide
- Transportation Cybersecurity Incident Response and Management Framework
- Autonomous Ground Vehicle Security Guide
- Cybersecurity Best Practices for the Safety of Modern Vehicles
- Cybersecurity Assessment Tool for Transit
- Sample Cybersecurity Clauses for EV Charging Infrastructure Procurements
- DOE Cybersecurity Strategy
- Cybersecurity Wargames for Small Intelligent Transportation Systems Teams
- Transportation Cybersecurity Resources

### Funding Programs, etc.

- State and Local Cybersecurity Grant Program
- Urbanized Area Formula Program
- Discretionary Grant Program

### Awareness Campaigns

- Vehicle Cybersecurity Training Curriculum Pilot Testing

# Ports and Maritime Transportation (shipping)

## Overview of Threats

In recent years, cyber threats in the port and maritime transportation (shipping) sector have skyrocketed due to heightened geopolitical tensions, affecting not only ports but also shipbuilders, IT providers, and vendors. Cyberattacks in this sector can have a variety of effects, including disruption of shipping and port operations, breaches to safety measures and systems, breaches to ships' communication and navigation systems, and cargo theft and associated economic losses. Disruptions to security systems, navigation, and communications can also lead to vessel accidents and result in injuries.

According to a study by NHL Stenden University in the Netherlands, there will be at least 64 cyber incidents worldwide in 2023, with most occurring in Europe and the Atlantic coast of North America, with incidents also confirmed in the Red Sea, Persian Gulf and East China Sea. About 80% of the attacks are from Russia, China, North Korea, and Iran.

While the port and shipping sector has taken measures on physical security challenges in the past, security measures in the digital realm are far from adequate. With the increasing digitization of ships and the widespread use of Internet devices at sea by low Earth orbit satellites, the increasing number of cyber attacks on ships' software update systems is of great concern to shipping operators.

## Relevant Authorities



USCG



MARAD



DOD



CISA

## Measures & Preparations

### Regulations

- Maritime Transportation Security Act: MTSA
- Executive Order on Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States
- Ocean Shipping Reform Act of 2023
- Final Rule: Cybersecurity in the Marine Transportation System

### Strategies & Guidelines, etc.

- Navigation and Vessel Inspection Circular (NVIC) 01-20, Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities
- Port Facility Cybersecurity Risks Infographic
- Maritime Cybersecurity Assessment and Annex Guide (MCAAG)
- Advisory: Maritime Port Vulnerabilities - Foreign Adversarial Technological, Physical, and Cyber Influence
- Marine Transportation System Resilience Assessment Guide (MTS Guide)
- MARAD Strategic Plan FY 2022 – 2026

### Funding Programs, etc.

- State and Local Cybersecurity Grant Program

### Awareness Campaigns

- The Coast Guard Maritime Industry Cybersecurity Resource website

# Water System

## Overview of Threats

Cyber attacks targeting water and wastewater systems are on the rise in the water supply sector. Water and wastewater systems increasingly rely on SCADA (Supervisory Control and Data Acquisition) systems to control and monitor water treatment plants, distribution networks, and wastewater facilities, and while these systems improve efficiency, they are vulnerable to cyber attacks. For example, if an attacker gains unauthorized access to the SCADA system and alters the operation of pumps, chemical dosing systems, water volume control, etc., the water supply can be disrupted, resulting in water quality degradation and overflow, posing a significant health risk to the public and potentially causing significant financial losses.

In October 2024, EPA released the results of a cybersecurity vulnerability inspection of drinking water systems across the U.S. that serve more than 3,300 people. The examination covered a total of 1,062 drinking water systems (serving more than 193 million people nationwide), and found that more than 70% of them did not fully meet cybersecurity requirements, and that 97 drinking water systems that supply drinking water to a total of approximately 26.6 million people had cybersecurity vulnerabilities of "critical" or "high" risk (vulnerabilities were rated on a four-level scale: "critical," "high," "medium," and "low").

The EPA warned that cyberattacks in the water sector could affect public health and disrupt public services, and that cybercriminals could gain access to employee and customer information.



EPA



CISA

## Relevant Authorities

## Measures & Preparations

### Regulations

- Cyber Incident Reporting for Critical Infrastructure Act of 2022: CIRCIA

### Strategies & Guidelines, etc.

- EPA Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems
- Incident Response Guide for Water and Wastewater Systems Sector
- Top Cyber Actions for Securing Water Systems
- Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems

### Funding Programs, etc.

- State and Local Cybersecurity Grant Program
- Clean Water State Revolving Fund (CWSRF)
- Midsize and Large Drinking Water System Infrastructure Resilience and Sustainability Program

### Awareness Campaigns

- EPA's Water Sector Cybersecurity Evaluation Program
- Cybersecurity Training



# Dams

## Overview of Threats

No cases of cyberattacks in the dam sector in the U.S. have been reported since 2013, according to public information. However, cyber attacks targeting dams can have wide-ranging effects, such as power outages, flooding, water supply disruptions, and reduced safety and economic damage to facilities and watershed communities. Therefore, it is important to strengthen cybersecurity.

There are more than 90,000 dams in the U.S., of which approximately 65% are privately owned and 31% are owned by governments, including federal and state governments. The Federal Energy Regulatory Commission (FERC) oversees approximately 2,500 hydroelectric dams (3% of the total number of dams).

The majority of dams in the U.S. are under the control of state and local governments or private entities, and the lack of uniform regulations is a challenge. Even for dams under FERC's supervision, lack of funding and staffing hinders the implementation of security measures

## Relevant Authorities



USACE



FERC



CISA

## Measures & Preparations

### Regulations

- Federal Energy Regulatory Commission Division of Dam Safety and Inspections FERC Security Program for Hydropower Projects Revision 3A
- Security Letter

### Strategies & Guidelines, etc.

- Dams Sector Cybersecurity Framework Implementation Guide
- Dams Sector Crisis Management Handbook
- Dams Sector Cybersecurity Capability Maturity Model (Dams-C2M2)
- Dams Sector Cybersecurity Capability Maturity Model (C2M2) Implementation Guide

### Funding Programs, etc.

- State and Local Cybersecurity Grant Program

### Awareness Campaigns

- FERC-D2SI Security Branch Webinar
- Sample Security Plan
- Homeland Security Information Network-Critical Infrastructure (HSIN-CI) Dams Portal



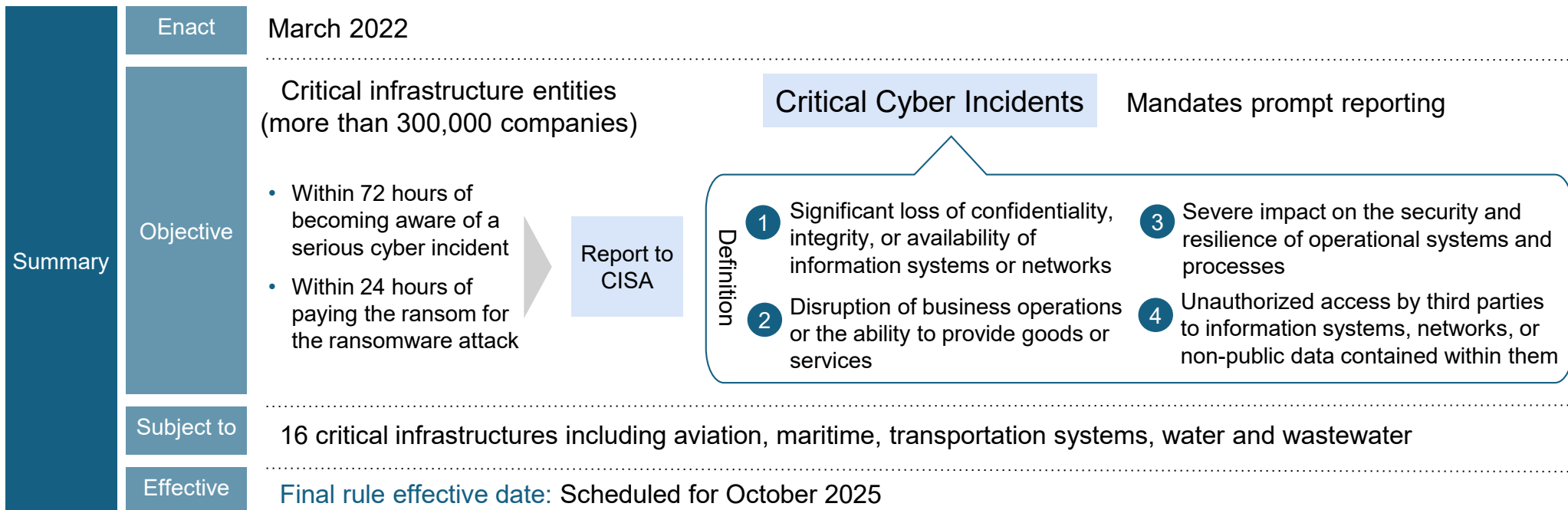
# Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) (scheduled to take effect in 2025)

In the United States, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) was enacted in March 2022, establishing legal frameworks and information-sharing provisions related to cyberattacks on critical infrastructure. On March 29, 2024, a proposed rule for the implementation of this law was announced, with the final rule expected to be finalized and take effect in October 2025.








This proposed rule requires businesses operating in 16 critical infrastructure sectors, including dams, transportation systems, and water supply systems (affecting over 300,000 companies), to report "significant cyber incidents" within 72 hours of detection and to report ransomware payments within 24 hours to the Cybersecurity and Infrastructure Security Agency (CISA).

Among various types of cyberattacks, ransomware poses the greatest threat to U.S. businesses, accounting for 47% of all cyberattacks in 2023.

The proposed rule has faced strong opposition from industry groups due to its burdensome burden obligations and ambiguous definitions.



In the United States, each industry sector has an ISAC to collaborate within the industry in the area of cybersecurity to address industry-specific issues. These ISACs focus on incident information sharing, best practices, and workforce development, aiming to enhance cybersecurity at the industry level.

Industry-Specific ISACs	Organization	Activities
Aviation ISAC	 <p>Based in Annapolis, Maryland, the organization was founded in 2014 with the goal of creating a more resilient global air transportation network. Aviation ISAC and its members work together to prevent, detect, respond to, and remediate cyber risks through threat intelligence sharing and best practices</p>	<ul style="list-style-type: none"> <li>(1) Information sharing and analysis</li> <li>(2) Development of best practices</li> <li>(3) Hosting events for knowledge</li> <li>(4) Strengthening partnerships</li> </ul>
Marine Transportation System ISAC	 <p>Established in February 2020 by U.S.-based maritime critical infrastructure stakeholders, this group plays a key role in coordinating timely, actionable cyber threat intelligence sharing. Its efforts focus on sharing IT, OT, and IoT system data to help stakeholders prevent or minimize cyber incidents.</p>	<ul style="list-style-type: none"> <li>(1) Information sharing</li> <li>(2) Training and awareness enhancement</li> <li>(3) Hosting events</li> </ul>
Real Estate ISAC	 <p>Founded in 2014 in Washington, D.C., the organization's role is to share and analyze information on cybersecurity threats and vulnerabilities in the real estate industry to raise awareness and strengthen collaboration on industry-specific security risks.</p>	<ul style="list-style-type: none"> <li>(1) Information sharing</li> <li>(2) Analysis and alerts</li> <li>(3) Collaboration</li> </ul>
Ground Transportation ISAC	 <p>Founded in 2002 in Washington, D.C., this organization enhances cybersecurity in truck and freight rail industries. It supports members in tackling security challenges, making informed decisions, mitigating cyber and physical threats, and exploring emerging trends to strengthen ground transportation security.</p>	<ul style="list-style-type: none"> <li>(1) Community support</li> <li>(2) Information sharing</li> <li>(3) Expert analysis and support</li> </ul>
Public Transportation and Express Bus ISAC	 <p>Founded in 2004 in Washington, D.C., and operated by the American Public Transportation Association (APTA), this organization supports public transit operators and industry stakeholders. It provides information and advisory services on physical and cybersecurity threats, vulnerabilities, and solutions to enhance security measures.</p>	<ul style="list-style-type: none"> <li>(1) Community support</li> <li>(2) Information sharing</li> <li>(3) Provision of expert analysis</li> </ul>
Automobile ISAC	 <p>Established in August 2015 by 14 automakers, including GM, Ford, and Toyota, this global information-sharing community focuses on connected car cybersecurity. Fully operational since January 2016, it serves as a central hub for sharing, tracking, and analyzing cyber threats, vulnerabilities, and incidents.</p>	<ul style="list-style-type: none"> <li>(1) Information sharing</li> <li>(2) Intelligence report creation</li> <li>(3) Workshops and events</li> <li>(4) Development of best practices</li> </ul>
Water ISAC	 <p>Founded in 2001 in Washington, D.C., the organization aims to strengthen security in the water and wastewater treatment sector by collecting and analyzing information on cyber-attacks and physical threats, and working to enhance cyber-security throughout the industry.</p>	<ul style="list-style-type: none"> <li>(1) Information gathering and analysis</li> <li>(2) Provision of tools</li> <li>(3) Education and information</li> </ul>



# Overview of U.S. Policy for In-House Production in the Infrastructure Sector

## Background

### U.S. Administration Policy

#### Objective

- Promotion of domestic manufacturing
- Job creation
- Economic growth

- Under the Buy American Act (enacted in 1933), the U.S. government sets and strengthens domestic production requirements for federally procured goods, aiming to achieve a “Made in America” policy in infrastructure projects.
- In January 2021, the Biden administration signed an executive order to reinforce the Buy American Act provisions, reaffirming its commitment to prioritizing domestic manufacturing.

## Main Policies

### Infrastructure Investment and Employment Law (BIL Law, enacted November 2021)

- The U.S. is investing in infrastructure, including roads, bridges, ports, airports, and railways.
- Under the Bipartisan Infrastructure Law (BIL), the Build America, Buy America Act (BABA) mandates U.S.-made steel, manufactured products, and construction materials for federally funded projects..

### Strengthening Domestic Production Requirements

- March 2022: DOD, GSA, and NASA raised the domestic production requirement for steel and other materials from 55% to 60% (increasing to 65% in 2024 and 75% in 2029).
- October 2024: FAR proposed removing 70 of 109 exempted items from domestic production requirements.
- January 2025: FHWA announced full enforcement of domestic requirements for highway projects.

## Promote Domestic Production

### Key Products Promoted for Domestic Production

- Batteries (for EVs and other electronic devices)
- Highways
- High-speed rail
- Ships
- Port cranes

#### Law

- Energizing American Shipbuilding Act of 2023
- Made in America Shipbuilding Act of 2020

### Promotion of shipbuilding industry

#### Partnership

- The U.S. is seeking partnerships with South Korea and Japan to strengthen its shipbuilding capacity.
- In December 2024, South Korea's Hanwha Group acquired Philly Shipyard for \$100 million.

## International Criticism (WTO Disputes)

- China: In 2024, requested WTO dispute settlement consultations, claiming the IRA tax credit requirements violate WTO rules.
- EU: Criticized the IRA's local content requirements and is considering WTO dispute settlement consultations.

# Trends and Policies Related to Other Economic Security Areas in the U.S. Infrastructure Sector

The U.S. employs laws, executive orders, regulations, tariffs, and foreign investment oversight to protect critical infrastructure from specific countries.

## Major Regulations and Initiatives

### Foreign Investment Committee to the U.S. (CFIUS) Regulation of Transactions for Economic Security

- The U.S. reviews foreign investments and certain real estate transactions for national security risks.
- In November 2024, the Treasury Department (USDT) issued a final rule strengthening CFIUS procedures, penalties, and enforcement powers.

### Efforts to Strengthen Cyber Security in Submarine Cables

- In April 2020, a presidential order established Team Telecom, an interagency group advising the FCC on telecom license reviews.
- It reviews foreign investments in U.S. telecom infrastructure, assesses national security risks, and examines submarine cable landing permits.

## Policies in the Maritime Transportation Sector

### Merchant Marine Act of 1920 (Jones Act)

- Enacted to maintain a strong commercial fleet that can support the Navy during war or national emergencies.
- Regulates maritime trade within U.S. waters and between U.S. ports.

### Maritime Security Program (MSP)

- Enacted to maintain a fleet of militarily useful commercial vessels.
- In a national emergency, these ships are immediately available to the DOD and must meet specific U.S.-flagged vessel requirements.

### SHIPS for America Act

- Proposed to reduce reliance on foreign ships and strengthen the U.S. supply chain.
- Aims to add 250 U.S.-built, U.S.-flagged international vessels with American crews within 10 years.

## Proposed Section 301 Measures Against China

- In February 2025, USTR proposed Section 301 measures, citing China's monopolistic practices in maritime, logistics, and shipbuilding as a U.S. trade threat.
- The plan includes port entry fees for Chinese shipping operators and Chinese-built vessels.

## Measures Against Chinese Cranes

- In February 2024, the USCG announced cyber risk management measures for owners and operators of Chinese-made cranes.
- Chinese-made cranes dominate the global market and account for about 80% of U.S. port cranes, with a high risk of remote unauthorized access.

## Exclusion Regulations

- **Entity List**
  - Published by the Bureau of Industry and Security (BIS), identifying entities engaged in activities contrary to U.S. national security or foreign policy interests.
- **List of Chinese Military Companies (CMC)**
  - Issued by the DOD, listing China-based firms operating in the U.S. with alleged ties to the Chinese military.



# Future Outlook

## Policy Recommendations for the MLIT

### Deepening Research on U.S. Best Practices

- Track updates on regulations and guidelines
- Research the U.S. audit framework, including staffing and audit scope
- Conduct interviews and site visits at U.S. public institutions impacted by cyberattacks to gather best practices

### Strengthen Information Sharing Between Japan and the U.S.

- Promote sharing of cyber threat intelligence and cybersecurity best practices
- Establish a framework to enhance U.S.-Japan information sharing.

### Strengthening Public-Private Partnerships

- Public and private sectors will work together to strengthen cybersecurity of critical infrastructure

## Recommendations for ISAC Efforts in Japan

### Strengthen Public-Private Partnerships and Activities

- Strengthen existing ISAC efforts while leveraging U.S. ISAC best practices.
- Conduct interviews and site visits at U.S. ISACs to gather detailed insights for Japan's ISAC development.
- Enhance collaboration and activities between Japan's ISACs and federal agencies.

### U.S.-Japan ISAC Collaboration

- Collaboration between Japan and U.S. ISACs is expected to be effective.
- Learning from U.S. cybersecurity best practices will help enhance Japan's industry capabilities.

### Clarification of Roles and Functions of ISAC

- Clarify the roles of ISACs and CEPTOAR and assess their collaboration framework.

## Key Considerations and Potential Opportunities for Japanese Companies in Overseas Infrastructure Expansion

### Policy Response to U.S. Domestic Production in Infrastructure

#### Utilizing and tracking exemptions

- Utilize exemption measures
- Prepare for post-exemption removal

#### Bilateral negotiations

- Negotiate a bilateral procurement agreement with the U.S

### Business Opportunities in Economic Security

#### Business expansion with strengthened ally cooperation

- Partner with U.S. firms in manufacturing.
- Monitor U.S. partnerships with other countries.
- Maintain dialogue with government officials.

#### Regulatory Compliance

- Understand and comply with U.S. regulations and guidelines

### Track Infrastructure Policies Under the Trump Administration

#### Track policy shifts and consider diverse infrastructure projects

- Monitor policy changes, cancellations, and new initiatives.
- Explore diverse infrastructure projects beyond federal funding reliance.