SECURE TOMORROW SERIES

OVERVIEW

The Cybersecurity and Infrastructure Security Agency's (CISA) Secure Tomorrow Series is a strategic foresight capability that examines emerging and evolving risks that could significantly affect our nation's critical infrastructure in the next three to seven years. Secure Tomorrow Series strives to build a more resilient and secure future by bringing together groups of subject matter experts (SMEs), thought leaders, and other stakeholders from diverse backgrounds to think proactively about future risks. Identifying these risks is essential to mitigating them before they affect critical infrastructure systems.

USING STRATEGIC FORESIGHT TO SECURE NATIONAL CRITICAL FUNCTIONS

A central premise of strategic foresight is that no one entity can successfully predict the future. Instead, the methodology treats the future as a set of plausible alternatives with the intent of identifying actions that, if taken today, would steer a community toward its preferred future. For CISA, this means a future in which the nation's critical infrastructure and the related National Critical Functions (NCFs) are more secure and resilient. In its role of identifying and reducing future risks, CISA's National Risk Management Center (NRMC) applies strategic foresight to identify risk mitigation strategies that are robust against uncertainty and uses this knowledge to promote methods for securing critical infrastructure systems that underpin the NCFs in the long term.

Secure Tomorrow Series efforts align with the NCFs approach to risk management. The NCFs are those functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

SECURE TOMORROW SERIES TOPICS OF EXPLORATION

For each phase of the Secure Tomorrow Series, CISA identified a set of topics that are likely to influence multiple NCFs. The current phase focuses on developing thinking around how the following three topics might affect critical infrastructure and cybersecurity:

Advanced Manufacturing

The world has seen steady growth in the industrial internet of things, 3D printing, and the power of information and big data analytics in manufacturing. The remainder of this decade will likely see the continued maturation and convergence of these areas, which will introduce a range of vulnerabilities and possible disruptions to critical infrastructure systems. Integrated cyber-physical systems, data-based semi-autonomous networks, and digital manufacturing processes make almost anything in a decentralized manufacturing ecosystem vulnerable to cybersecurity attack or manipulation from malicious actors. Moreover, the expansion of advanced manufacturing processes for biological and medical purposes raises questions about toxicity, the biocompatibility of manufactured parts, and nefarious applications. In addition, supply chain risks and workforce challenges threaten the U.S. outlook on advanced manufacturing.
NCFs include: Manufacture Equipment, Provide Information Technology Products and Services, Protect Sensitive Information, Produce Chemicals, Provide Metals and Materials, Research and Development, and Educate and Train

Information and Communications Technology (ICT) Supply Chain Resilience

Managing risk in the ICT supply chain is an evolving challenge that spans multi-billion-dollar black markets, geopolitical tensions, and rapid technological change. Present-day challenges such as counterfeit components and the need for

effective international standards are likely to grow this decade. Evolving future challenges such as the rollout of 5G, the proliferation of artificial intelligence–enabled cyber weapons, and the increasing instability in domestic energy infrastructure will each add new layers of complexity to ICT supply chain risk management. These challenges will necessitate stronger governance and visibility, improved information sharing among relevant parties, and better training for those directly involved in the ICT supply chain.
NCFs include: Provide Wireless Access Network Services; Provide Internet Routing, Access, and Connection Services; Provide Internet Based Content, Information, and Communication Services; Operate Core Network; Provide Information Technology Products and Services; Perform Cyber Incident Management Capabilities; and Protect Sensitive Information

Water Availability

Water of sufficient quantity and quality is essential for human health, economic productivity, and the operation of critical infrastructure. Major climatic, demographic, economic, and policy pressures on water resources will increase the risks of water shortages and rising water prices in the near term. In the long term, these pressures potentially will alter agricultural growing areas, damage ecosystems, disrupt water transportation routes, generate acute health crises, increase inequities in water access, and contribute to failures of water and wastewater infrastructure. The interconnected nature of water with food and energy ensures that disruptions in water availability will lead to a wide range of cascading effects throughout critical infrastructure sectors.
NCFs include: Supply Water, Manage Wastewater, Produce and Provide Agricultural Products and Services, Maintain Supply Chains, Generate Electricity, Support Community Health, Transport Cargo and Passengers by Vessel, and Exploration and Extraction of Fuels

SECURE TOMORROW SERIES TOOLKIT

In November 2022, CISA began conducting research on each topic and engaging with SMEs from academia, think tanks, the private sector, and the U.S. Department of Energy's National Labs to develop knowledge products meant to encourage systems thinking; identify emerging risks; develop corresponding risk management strategies to implement now; and stress-test these strategies against multiple alternative futures.

One of the key knowledge products is the Secure Tomorrow Series Toolkit. The toolkit consists of supporting materials (e.g., facilitation guides, scenarios, game components) to help critical infrastructure stakeholders and planning communities' organizations conduct strategic foresight activities, support strategic planning, and be empowered to execute these methods to examine the three topics. Toolkits for previous phases are available for download on NRMC's webpages on CISA.gov or by scanning the QR code shown below.

RESOURCES

- National Risk Management: CISA.gov/national-risk-management
- National Critical Functions: CISA.gov/national-critical-functions
- Secure Tomorrow Series: CISA.gov/secure-tomorrow series
- Secure Tomorrow Series Toolkit: CISA.gov/secure-tomorrow-series-toolkit

For more information, contact us at SecureTomorrowSeries@cisa.dhs.gov.

Scan this QR to go to the webpage directly.