SECURE TOMORROW SERIES CROSS-IMPACTS READ AHEAD: ICT SUPPLY CHAIN RESILIENCE

CROSS-IMPACTS SESSION

In this facilitated activity, participants will brainstorm how six drivers of change in the resilience of the information and communications technology (ICT) supply chain might affect seven National Critical Functions (NCFs).[1] Specifically, participants will identify critical infrastructure[2] risks related to ICT supply chain resilience that they expect to see in the next three to seven years, determine which risks are unique to individual NCFs or specific critical infrastructure systems, and identify strategies to mitigate those risks.

No advance preparation is necessary. However, participants may wish to familiarize themselves with the drivers of change and NCFs that they will be "crossing" during the session. The intersection of a particular driver of change and NCF (i.e., what risks the driver of change poses to that NCF) forms the basis for discussions during the activity. Ultimately, participants will select six of these intersection points to focus on, based on a prioritization exercise at the start of the session.

Table 1 lists and briefly describes the six drivers of change that participants will choose from during the session.

Table 1: Drivers of change addressed in the cross-impacts session

Driver of Change	Description
Artificial intelligence	Includes malware enhanced for detection avoidance, lateral movement speed, obfuscation of command and control mechanisms, and efficient data exfiltration
Edge computing and software-defined networks	Includes the increased cyberattack surface of less centralized system architectures
Extent of globalization	Includes the ramifications of moving away from globalized supply chains to domestically controllable supply chains
Growing energy demands	Includes the challenges of managing the rapidly growing computing demand, as driven by Internet of Things and artificial intelligence
Internet standards	Includes the ramifications of receding U.S. influence in international bodies for setting internet standards
Third-party testing	Includes the consequences of compromised code being integrated into the ICT supply chain and the existence of an expansive black market for compromised physical components

[1] 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 national security, national economic security, national public health or safety, or any combination thereof.
[2] For a complete list and description of the 16 critical infrastructure sectors, see www.cisa.gov/critical-infrastructure-sectors.

Table 2 provides definitions for the seven NCFs addressed in the session. For additional information on all 55 NCFs, participants may wish to review National Critical Functions: Status Update to the Critical Infrastructure Community.

Table 2: NCFs addressed in the cross-impacts session

National Critical Function	Definition
Operate Core Network	Maintain and operate communications backbone infrastructure for voice, video, and data transmission that connects to users through broadcasting, cable, satellite, wireless, and wireline access networks
Perform Cyber Incident Management Capabilities	Provide security systems and services that protect critical business assets and functions, including preventive guidance, simulation, testing, and warning capabilities; operate operations response centers and teams; integrate and share information; coordinate and provide response, recovery, and reconstitution services
Protect Sensitive Information	Safeguard and ensure the integrity of information whose mishandling, spillage, corruption, or loss would harm its owner, compromise national security, or impair competitive or economic advantage
Provide Information Technology Products and Services	Design, develop, and distribute hardware and software products and services (including security and support services) necessary to maintain or reconstitute networks and associated services
Provide Internet-based Content, Information, and Communication Services	Produce and provide technologies, services, and infrastructure that deliver key content, information, and communications capabilities via the Internet
Provide Internet Routing, Access, and Connection Services	Provide and operate exchange and routing infrastructure, points of presence, peering points, local access services, and capabilities that enable end users to send and receive information via the Internet
Provide Wireless Access Network Services	Provide access to core communications network via electromagnetic wave-based technologies, including cellular phones, wireless hot spots (Wi-Fi), personal communication services, high-frequency radio, unlicensed wireless, and other commercial and private radio services

The Cybersecurity and Infrastructure Security Agency (CISA) has produced these scenarios to initiate and facilitate discussion. The situations described here are hypothetical and speculative and should not be considered the position of the U.S. government. All names, characters, situations, organizations, and incidents portrayed in these scenarios are fictitious. Any positions expressed by fictional characters herein regarding any particular issues or technologies do not represent the positions of CISA or the federal government.