SECURE TOMORROW SERIES CROSS-IMPACTS READ AHEAD: DATA STORAGE AND TRANSMISSION

CROSS-IMPACTS SESSION

In this facilitated activity, participants will brainstorm how drivers of change for **data storage and transmission** might affect different National Critical Functions (NCFs)[1] in distinct ways. Specifically, participants will seek to identify risks to critical infrastructure[2], organized around NCFs, related to data storage and transmission that we can expect in the next five years, make distinctions about which risks are unique to individual NCFs or specific critical infrastructure, 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 point of a particular "driver of change" and NCF—i.e., what risks does the driver of change pose to that NCF—forms the basis for discussions during the activity. Ultimately, participants will focus on six of these intersection points, which will be selected based on a prioritization exercise that they will conduct at the start of the session.

Table 1 lists the eight drivers of change that participants will choose from during the session and provides brief descriptions of each.

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

Driver of Change	Description
Increasing volume of data	To include ramifications arising from a projected near tripling of the data globally (to 175 zettabytes) from 2000 to 2025.
Inadequate access controls	To include challenges with appropriately restricting data access to only authorized users and the consequences of failures to do so in the future data environment
Reliance on cloud computing	To include the influence of shifts in data storage to the cloud and growing reliance on cloud service providers
Rise in the number of Internet of Things devices	To include the security implications arising from the proliferation of Internet of Things devices and sensors
Data management and quality issues	To include ramifications from deliberate or accidental undermining of data quality and integrity
Increasing number of cyberattacks & changing tactics	To include targets for cyberattacks and consequences of successful attacks in the future data environment
International competition/conflict	To include ramifications of competition between the U.S. and China and increasing desires for cyber independence in foreign countries
Remote work	To include the longer-term and cascading effects arising from large, rapid, and potentially permanent shifts to remote work catalyzed by the pandemic

[1] National Critical Functions 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 sixteen critical infrastructure sectors, see www.cisa.gov/critical-infrastructure-sectors.

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

Table 2. NCFs addressed in the cross-impacts session

National Critical Function	Definition
Provide internet based content, information, and communications 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
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
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
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 identity management and associated trust support services	Produce and provide technologies, services, and infrastructure to ensure the identity of, authenticate, and authorize entities and ensure confidentiality, integrity, and availability of devices, services, data, and transactions

Participants are reminded that any information shared during this activity is provided on a voluntary basis. Sensitive information, to include confidential or proprietary information, should not be shared. Information shared during this activity may be recorded for the purposes of facilitating the program and discussions; however, discussion or disclosure of information in these sessions is not a substitute for submission under the Protected Critical Infrastructure Information (PCII) Program. Information may therefore be subject to Freedom of Information Act (FOIA) requests or other mechanisms that would publicize any information shared and/or recorded.