SECURE TOMORROW SERIES CROSS-IMPACTS READ AHEAD: ANONYMITY AND PRIVACY

CROSS-IMPACTS SESSION

In this facilitated activity, participants will brainstorm how drivers of change for **anonymity and privacy** might affect different National Critical Functions (NCFs)[1] in distinct ways. Specifically, participants will seek to identify risks to critical infrastructure, organized around NCFs, related to anonymity and privacy 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 seven 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
Improper security protocols	To include ramifications from the combination of increasing amounts of personal data being collected by organizations (as a prerequisite to receiving services and/or personalized products) and inadequate safeguarding of that data
Ubiquitous and unregulated data collection, brokering, and aggregation	To include risks arising from monetization of user data and an environment in which data brokers can effectively sell, analyze, or manipulate user data without restrictions and without user consent or knowledge
Abuse of user data sharing practices	To include how malicious actors are, without the consent or knowledge of users, collecting users' online activity (particularly on social media), tracking them across various platforms, and manipulating their views through targeted messaging
Technological advancements	To include ramifications of advances in machine learning, artificial intelligence, supercomputing, and other technologies for circumventing current data anonymization methods that protect user privacy
Legislation	To include challenges and risks presented by the current U.S. regulatory environment for data privacy (and the absence of a comprehensive U.S. data privacy law) and foreign data privacy regimes
Insufficient data governance	To include how a lack of or insufficient data governance can prevent an organization from successfully implementing their privacy strategy and can exacerbate privacy risks
Information technology/operational technology (IT/OT) convergence	To include the security risks posed by critical infrastructure systems that increasingly connect their physical assets to the internet (e.g., internet of things or "smart" devices)

[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.

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
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
Preserve constitutional rights	Secure the principles of freedom and independence and maintain the structures of American government through the protection of rights and processes prescribed in the U.S. Constitution
Enforce law	Operate federal, state, local, tribal, territorial, and private sector assets, networks, and systems that contribute to enforcing laws, conducting criminal investigations, collecting evidence, apprehending suspects, operating the judicial system, and ensuring custody and rehabilitation of offenders
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, authenticity, and authorization of entities and ensure the confidentiality, integrity, and availability of devices, services, data, and transactions
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

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.