SECURE TOMORROW SERIES CROSS-IMPACTS READ AHEAD: QUANTUM TECHNOLOGIES

CROSS-IMPACTS SESSION

In this facilitated activity, participants will brainstorm how drivers of change for quantum technologies might impact our Nation's critical infrastructure in the future by using the National Critical Functions (NCFs)[1] framework to identify and analyze risk. Specifically, participants will seek to identify risks to critical infrastructure[2], organized around NCFs, related to quantum technologies that we can expect in the next 10 to 15 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 the driver of change poses 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 a brief description of each.

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

Driver of Change	Description
Advances in quantum communications	To include challenges associated with quantum key distribution, quantum repeaters, quantum communication, and quantum networks
Advances in quantum computing	To include threats and opportunities arising from the development of sufficiently powerful quantum computers
Advances in quantum sensors	To include the security implications arising from lower cost, smaller quantum sensors that feature better sensitivity and spatial resolution than other sensors
Data harvesting	To include ramifications of adversaries collecting and storing encrypted data for eventual decryption when a sufficiently powerful quantum computer is realized
Reliance on digital signatures	To include society's growing dependence on technologies (e.g., blockchain, Internet of Things devices) that use digital signatures and their role in smart cities
Synergies and virtuous cycles	To include potential interactions between quantum technologies and other technologies and virtuous cycles for first movers in applying quantum computing to solve problems

[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.

Timeline uncertainty	To include the ramifications of faster-than-anticipated developments in quantum technologies for transition to a postquantum cryptographic era

Table 2 provides definitions for the six 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
Conduct elections	Conduct elections, including managing voter registration and rolls, voting infrastructure, polling places, vote counting, and certifying and publishing election results
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 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
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 communications services	Produce and provide technologies, services, and infrastructure that deliver key content, information, and communications capabilities via the Internet
Research and development	Conduct basic research, innovate, test, and introduce new products and services or improve existing products and services

Participants are reminded that any information shared during this activity is provided on a voluntary basis. Sensitive information, including 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 Program. Information may therefore be subject to Freedom of Information Act requests or other mechanisms that would publicize any information shared or recorded.