# SECURE TOMORROW SERIES CROSS-IMPACTS READ AHEAD: BRAIN-COMPUTER INTERFACES

## CROSS-IMPACTS SESSION

In this facilitated activity, participants will brainstorm how drivers of change for brain-computer interfaces (BCIs) 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 BCI 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 eight 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 "reading" data from the brain | To include ramifications emerging from advances in reading brain signals and decoding these signals with greater speed and accuracy |
| Advances in "writing" data to the brain | To include ramifications emerging from the ability to transmit and implant information directly to the brain |
| Commercial influences | To include emerging commercial use cases for BCIs and resultant implications for cybersecurity and neurodata consumption, monetization, and privacy |
| Ethical and accountability concerns | To include consequences of failing to establish and ensure neuro-rights and resolve questions about personal accountability |
| Harmful effects | To include hypothetical means of harming individuals through BCIs (e.g., mental damage, influencing behavior, sabotage) or using BCIs to control devices that would facilitate attacks |
| Inequities in access | To include how society and critical infrastructure systems will address challenges arising from disparate access to BCI technologies |

[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.

| | |
|---|---|
| **International competition** | To include implications of market dominance by and dependence on a foreign nation related to BCI |
| **Performance augmentation** | To include the potential disruptions introduced by applying BCI technologies in ways ranging from enhancing attention to human-machine teaming |

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 |
|---|---|
| **Educate and train** | Provide education and workforce training including Pre-K–12, community college, university, and graduate education, technical schools, apprenticeships, non-formal education, and on-the-job training |
| **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 |
| **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 medical care** | Ensure the provision of healthcare services |
| **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 |
| **Support community health** | Conduct epidemiologic surveillance, environmental health, migrant and shelter operations, food establishment inspections, and other community-based public health activities |

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.