SECURE TOMORROW SERIES CROSS-IMPACTS READ AHEAD: ADVANCED MANUFACTURING

CROSS-IMPACTS SESSION

In this facilitated activity, participants will brainstorm how seven drivers of change for advanced manufacturing might affect seven National Critical Functions (NCFs).[1] Specifically, participants will identify critical infrastructure[2] risks related to advanced manufacturing 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 seven 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
Bioengineering	Includes the ramifications of advances in manufacturing for biomedical uses and the ability to ensure appropriate quality assurance and safety standards
Capability access	Includes the ramifications of potentially uneven adoption of and access to advanced manufacturing capabilities, including resultant effects on U.S. competitiveness
Cybersecurity	Includes exploiting vulnerabilities to weaponize or sabotage 3D printed materials and gain access to and damage the broader manufacturing ecosystem, as well as risks arising from increasing use of digital threads and digital twins in manufacturing processes
Heterogeneity	Includes risks arising from the proliferation and integration of various advanced manufacturing technologies (e.g., cloud computing, industrial Internet of Things, and information technology and operational technology convergence)
Insufficient governance	Includes potential consequences arising from the absence of transparency and government oversight related to advanced manufacturing standards and regulations

[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.

Sustainability	Includes the supply chain, scalability, and quality challenges in the development of efficient advanced manufacturing prototype and automation processes
Workforce disruption	Includes the potential challenges in applying or managing advanced manufacturing technologies in ways ranging from enhanced workplace visualization methods to human-machine teaming

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
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
Manufacture Equipment	Fabricate and assemble components to produce tangible property
Produce Chemicals	Manufacture basic chemicals from raw organic and inorganic materials and manufacture intermediate and final products from basic chemicals
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 Metals and Materials	Manufacture iron, steel, and ferro-alloy products; alumina and aluminum products; non-ferrous metals; and other materials as primary components for other industries
Research and Development	Conduct basic research, innovate, test, and introduce new products and services or improve existing products and 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.