

National Commission on Innovation & Competitiveness Frontiers

Key Takeaways from 2024 Working Groups



Working Group 2

The Future of Technology: Developing and Deploying Disruptive Technologies at Scale

Session 4: June 4th, 2024

This Working Group session focused on enhancing security and reliability in critical supply chains and our research ecosystem.

I. KEY THEMES

Working Group discussion identified several key themes during this session:

- 1) **Cross-cutting federal policy actions** can support the structures and processes underpinning a secure supply chain and research ecosystem.
- 2) **Secure ecosystems require secure data.** Effective data security infrastructure, guidelines, and standards will allow for innovation to thrive in a secure environment.
- 3) **Securing critical supply chains** requires a targeted policy focus, including new, tailored programs.
- 4) **Consortium building between public and private partners** will help regional supply chain ecosystems to be more robust, reliable, and resilient to disruptions.

II. PRELIMINARY IDEAS & POTENTIAL RECOMMENDATIONS

Cross-cutting federal policy actions

- A secure research ecosystem is built on secure infrastructure. In many areas of the country, there is an opportunity to create secure research facilities that can advance technologies essential to our economic and national security. However, the process to approve and build these facilities is inordinately long; to begin a conversation on needs and capabilities with the Defense and Counterintelligence Security Agency, the waiting list is over 18 months. Particularly in areas such as critical minerals and specialty manufacturing, the timeline to construct new secure research facilities must be accelerated.

- The stubbornly slow permitting process in the U.S. hurts our ability to build up domestic supply chains, especially for the mining and processing of critical minerals. Federal action is needed to speed permitting processes for essential inputs to emerging technologies.
- As many supply chains are re-shored and domestic manufacturing capacity grows, workforce demands will become even more acute. Policymakers should retool the federal workforce development apparatus to speed the creation of talent in areas such as manufacturing and micro-technologies. To create integrated supply chains with reliable regional suppliers, special attention should be paid to further developing rural workforces.

Secure ecosystems require secure data

- Open-source software enables efficient and flexible operations while allowing for continued innovation, particularly in the field of supply chain logistics. However, it also opens vulnerabilities to cyberattacks and data breaches, which can endanger the security and integrity of supply chains in critical technologies. Federal standards, guidelines, and tools for digital provenance are needed to secure supply chain data ecosystems and enable trust and validation across a wide range of software use cases.
- Secure and trusted data ecosystems enable collaboration, especially with international partners. While public and private partners abroad can be valuable collaborators, international engagement cannot compromise confidential data on supply chains and research. The federal government should reinforce research integrity and data integrity principles and norms, including implementing recommendations in the JASON report on research security. This effort will require international coordination and strong U.S. leadership, but should not require significant funding, marking it as a high-value priority.

Securing critical supply chains

- Certain supply chains merit a targeted policy focus to ensure their strength and integrity, based on the impact to economic and national security. Specific areas include semiconductors, AI, batteries, hypersonics, and feedstocks for the chemical and agricultural industries. However, this list is not exhaustive, and should be expanded to any area with significant security implications.
- Each critical technology and essential industry should have a dedicated national program for supply chain strengthening. As many competitors, including China, undertake nationally coordinated actions to rapidly expand their supply chains, the U.S. becomes at risk of falling behind. The federal government should create, fund, and codify national programs for specific technologies and industries, aligning each program through a national supply chain strategy.

- Securing critical supply chains requires better knowledge and data around supply chain activities at national, regional, and local levels. The OECD has created a digital inventory of all major health issues, allowing for a broad variety of actors to understand and act on health issues. The U.S. needs similar tools for states, regions, and the nation to predict and proactively address supply chain issues. Data creation and active monitoring efforts should be run out of a national office to allow for maximum interagency data sharing, state and regional coordination, and national reach.
 - One approach participants discussed was a digital twin, detailing the location and amount of various inputs in the supply chain. Digital twins can help predict supply shortages and test millions of scenarios to inform better planning. However, digital twins may not be best suited for all technology areas, and raises questions of data ownership and compensation for data sharing.
 - Participants emphasized the value of artificial intelligence (AI) in supply chain analytics. AI can help evaluate the current state of supply chains, but is particularly valuable in modelling and forecasting needs and shortages in certain sectors. However, more data is needed to enable system-wide supply chain evaluation and forecasting.

Consortium building between public and private partners

- To build an integrated supply chain, it is necessary to establish partnership and coordination between different members of the ecosystem. This includes not only suppliers and vendors, but also the companies and organizations demanding inputs, universities and laboratories conducting basic and applied research, local communities underpinning a strong workforce, and policymakers leading supply chain strategies.
- A consortium approach, in which a wide variety of stakeholders can collaborate towards a clear goal, will best enable an integrated supply chain ecosystem. The diversity of partners also helps to make supply chain strengthening efforts more resilient to swings in federal policy and funding.
- To ensure the continued growth of emerging technology hubs, potential supply chain weaknesses should be predicted and proactively addressed. For example, the Minneapolis region has become a hub for medicine and bioscience, building a robust vendor and supplier network within the region. However, most inputs to pharmaceuticals and medical device components come from Asia and other parts of the world, leaving the supply chain vulnerable to disruptions. For this technology hub to continue expanding, and to increase its sustainability, security, and resilience, the region will need to rapidly develop alternate supply chains.
- As regional consortia form and grow, there are opportunities for partnerships to open new collaborations and impact policy decisions. By integrating regional systems,

consortia can learn from one another and find common ground on policy priorities – leveraging a variety of experiences and strategies to inform federal policymaking on innovation and competitiveness. Organizations like the Council on Competitiveness can serve as system integrators, facilitating collaboration between regional consortia.