# Principles for Improved Policymaking and Enhanced Cooperation on National Security, Technology, and Trade

June 2020

ITI

Promoting Innovation Worldwide

The global tech sector agrees that increased trade and innovation raise new types of national security risks and has a strong record of supporting U.S. national security. It is concerned, however, that the U.S. government is moving to address these very legitimate risks in ways that could create unintended negative consequences for U.S. competitiveness, technological leadership, and – ironically – national security.

It is essential that the U.S. government and global companies work together to meet these challenges in ways that draw on the United States' technological leadership, economic openness, and strong alliances. Now more than ever, the United States' ability to protect its national interests depends on harnessing its economic and business strengths, its still significant diplomatic clout, and its unrivaled instinct for innovation.

ITI and its member companies support U.S. government efforts to find the right policies to address these new types of risks. The following Principles for Improved Policymaking and Enhanced Cooperation on National Security, Technology, and Trade can serve as a roadmap for national security policymaking that focuses on targeted solutions, enhances cooperation between government and industry, and plays to the United States' historical strengths in innovation, business, and international cooperation.

# Principles for Improved Policymaking and Enhanced Cooperation on National Security, Technology, and Trade

Protecting national security is the most important responsibility of governments. It is the foundation for political freedom, economic opportunity, and the rule of law, enabling companies to innovate, create jobs, and support the industrial base. In an increasingly digital world, technology and business are evolving in ways that make national security a truly shared responsibility between government and industry. It has never been more important for the U.S. government and global companies to work together, across the full spectrum of public and private technologies, to harness U.S. technological leadership, economic openness, and international engagement in order to strengthen national security. The below principles provide a "north star" for both government and industry to do so.

## 1 Effective national security requires technological leadership.

Technological leadership – the extent to which the United States is at the cutting edge of developing and commercializing the technologies of the future – drives U.S. innovation, job creation, and economic growth, which are essential to U.S. national security. Public and private sector commitments to research and development, public policies that attract and reward human talent, and economic frameworks that allow companies to freely operate and innovate all help ensure that the benefits of technology flow to the U.S. industrial and defense base. The U.S. government should design and deploy national security tools in ways that support companies in driving innovation and that promote, rather than impede, U.S. technological leadership.

## 2 Technological leadership depends on economic openness.

International trade and investment not only enhance the ability of companies to grow and compete; they also contribute to U.S. technological leadership. Access to export markets allows firms to increase sales and profitability, which enables them to further invest in innovation in the United States and drive standards development around the world. Support for secure global supply chains, where companies have strong track records for security and cooperation with like-minded economies, allows companies to reduce costs and increase productivity. Openness to trusted foreign investment allows the U.S. economy to create American jobs, increase U.S. tax revenue, and support domestic R&D. The U.S. government should advance trade and investment policies that allow companies to succeed commercially and thereby contribute to technological leadership and economic competitiveness.

## 3 National security measures should focus on identified national security risks.

The majority of technology-related business activities presents no national security concerns. Overbroad policy responses risk stifling innovation, hindering technological leadership, and harming the industrial and defense base. The U.S. government should take a rigorous and targeted approach to addressing technology-related (and other) national security concerns, ensuring that laws, regulations, and other measures: (a) are based on factual evidence of concrete risks; (b) are narrowly-tailored to the risks themselves, rather than applied to entire categories of technology or business activity; (c) seek, where possible, to mitigate risks rather than prohibit business activity; (d) are not used to advance trade or other economic policy goals; and (e) otherwise avoid creating unnecessary costs, regulatory burdens, or government expenditures.

## 4 The United States should work in concert with like-minded economies.

Given the constant cross-border flow of goods, services, and data, it is imperative that the U.S. government closely coordinate its technology-related national security policies with like-minded economies, such as the European Union, Japan, United Kingdom, South Korea, Canada, and Australia. Multilateral export controls, for example, help keep critical technologies out of the hands of hostile actors and support U.S. economic interests by avoiding the diversion of business to other markets. Similarly, U.S. participation in global, industry-led standard-setting organizations ensures that certain economies and companies do not exert undue influence on the direction of next-generation technologies. The United States and like-minded economies should take common approaches to technology-related national security risks – for example by ensuring expedited approvals of technology exports among such economies – to avoid harmful policy fragmentation and maximize the likelihood of achieving shared security objectives.

## 5 The U.S. government and industry should cooperate robustly and continuously.

Policymakers and companies each have important and distinct roles to play in addressing technology-related national security risks. The U.S. government has information that companies do not have about national security threats. Companies have information that governments do not have about their network operations and how they detect, manage, and defend against risks to data, systems, networks, and supply chains. Both policymakers and industry should communicate regularly and robustly about relevant risks (consistent with limitations relating to classified information and business confidentiality), including through opportunities for industry input in regulatory rulemaking processes, public-private task forces and other collaborative mechanisms, and informal relationships between policymakers and companies.