MIKE CRAPO
United States Senator

MICROCHIPS Act

The Problem:

The U.S. is involved in asymmetric warfare and what amounts to a technological space race with China, which is seeking to dominate an over $1.5 trillion electronics industry through state investment, subsidies and intellectual property (IP) theft. China has capabilities to undermine U.S. national security in four major non-kinetic areas with implications across the government: **supply chain exploitation** (e.g. supplying software and hardware with backdoor access or faulty component parts), **cyber-physical attacks on systems with real-time operating deadlines** (e.g. missiles, aircraft, electrical grids, etc.), **cyber-IT** (e.g. hacking of computer systems), and **human actors** (e.g. using insiders to gain sensitive information). China can and has used these types of attacks together as part of a blended national strategy to undermine the U.S.

While these threats have been largely acknowledged by the government, the U.S. still lacks a coordinated, whole-of-government strategy to address them, particularly supply chain exploitation. The lack of comprehensive detection and apprehension of potentially compromised technology and component parts has practical and serious implications. U.S. companies continue to lose billions of dollars of IP to theft by China. Additionally, counterfeit and compromised electronics installed in U.S. military, government and critical civilian platforms give China potential backdoors to interfere with and compromise these systems. Implications of an insecure U.S. supply chain extend beyond the government—any industry that relies on electronics for secure communication, data transfer, or operations is susceptible to attack through a compromised supply chain.

The Solution:

The Manufacturing, Investment, and Controls Review for Computer Hardware, Intellectual Property, and Supply **"MICROCHIPS" Act** would address this pressing challenge by leveraging government and private sector expertise to develop a national strategy and establishing a central clearinghouse for assessing risks to critical technologies, fortifying the industrial base against these threats, and preventing compromised materials from entering the U.S. supply chain.

Brief Section by Section:

- **Sec. 1** Short Title
- **Sec. 2** Findings and Sense of Congress.
- **Sec. 3** Directs the Director of National Intelligence, Department of Defense, and other relevant agencies to develop a plan to increase supply chain security and develop interagency sharing within 180 days.
- **Sec. 4** Establishes to establish a National Supply Chain Security Center within the Office of the Director of National Intelligence.
- **Sec. 5** Modifies the Defense Production Act to make supply chain security a purpose for investment.