Pacific Northwest
NATIONAL LABORATORY

PNNL-SA-173570

U.S.-China Competition in Global Supply Chains

Testimony before the U.S.-China Economic and Security Review Commission

June 2022

John VerWey - East Asia National Security Advisor

1. Key Concepts and Definitions

Different U.S. government agencies maintain different definitions of "supply chain" and various lists of "critical technologies."[1] I will discuss both of these concepts in detail later, but for the purposes of my testimony, when I refer to a supply chain I am talking about "a network of people, processes, technology, information, and resources that delivers a product or service."[2] When referring to critical technologies, I am generally referring to a range of technologies identified by the White House Office of Science and Technology Policy in February 2022.[3]

Supply chain risk management (SCRM) is the management of risk to the integrity, trustworthiness, and authenticity of products and services within a supply chain.[4] Historically the primary focus of SCRM has revolved around maintaining *cost*, *schedule*, and *performance*.[5] Private sector SCRM efforts prioritize delivery of products and services on time, at reasonable cost, and to specifications ("to spec"). However, for national security systems, SCRM also focuses on *security*. The term "security" encompasses concepts like trust, traceability, integrity, and resilience, among others. SCRM draws on many disciplines and requires participation from subject matter experts in acquisition, information assurance, logistics, analysis, and risk.[6]

At a very basic level, U.S. government SCRM efforts attempt to answer the question "can we trust who we're buying from to deliver products and services on time, at cost, to spec, securely?" Regardless of whether this question is answered affirmatively or negatively, the goal is to increase the overall resilience of the supply chain to prepare for unexpected events, respond to disruptions, and recover from them.[7] Answering this question for specific critical technologies can require access to high fidelity data, detailed supply chain mapping, technical expertise, ongoing monitoring and evaluation, and modeling. The fact that critical technology supply chains are often entirely commercial and outside government control and limited data is available at the multiple tiers of vendors located in adversary countries, makes this effort more complex and difficult.

"Tiers" refer to different levels in a supply chain. Supply chain tiers are easily understood by thinking about aircraft manufacturing. A plane is provided by an original equipment manufacturer (OEM). This OEM relies on Tier 1 vendors to provide various components like wings, engines, avionics, and tires. Tier 1 vendors rely on Tier 2 vendors to supply subcomponents. For example, avionic suppliers rely on electronic assemblies. These Tier 2 suppliers rely on Tier 3 suppliers for items that go into electronic assemblies like printed circuit boards (PCBs) and integrated circuits (ICs). And these Tier 3 suppliers rely on Tier 4 suppliers for equipment used to fabricate PCBs and ICs. Finally Tier 4 suppliers rely on Tier 5 suppliers for raw materials like silicon. Mapping supply chains gets progressively more difficult the

---

[1] See Appendix A and F for representative examples.

[2] https://www.dni.gov/files/NCSC/documents/supplychain/20200925-NCSC-Supply-Chain-Risk-Management-tri-fold.pdf

[3] https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf

[4] https://www.dni.gov/files/NCSC/documents/supplychain/20190327-ICD731-Supply-Chain-Risk-Manage20131207.pdf

[5] https://www.dni.gov/files/NCSC/documents/supplychain/20190327-Deliver-uncompromised.pdf

[6] https://www.dni.gov/files/NCSC/documents/supplychain/20190327-ICD731-Supply-Chain-Risk-Manage20131207.pdf

[7] https://www.emerald.com/insight/content/doi/10.1108/09574090910954873/full/html.

"deeper" one looks into the tiers. Frequently, OEMs do not have good visibility in to their Tier 4 and Tier 5 suppliers.

Chinese firms are dominant in a wide variety of critical technology supply chains at various tiers. This dominance may range from obvious to opaque and requires careful analysis of upstream and downstream supply chains to correctly identify and map the tier in which their dominance is present. As will be discussed later, Chinese dominance is particularly acute in raw materials mining, refining, and processing, where the U.S. is 100% reliant on Chinese firms for supply of certain minerals.[8]

In the supply chain world, the concept of being 100% reliant on a particular firm for supply of a product or service makes that vendor a "sole-source supplier" or a "single-source supplier." A sole-source supplier is the only *known* vendor of a particular product or service. A single-source supplier is the only *qualified* vendor of a particular product or service. For many U.S. national security systems, there are single or sole-source suppliers present in various tiers of the supply chain. Single- and sole- source suppliers are among the most obvious and acute supply chain risks.

There are a wide variety of supply chain risks. Single- and sole- source suppliers are examples of market concentration risks, in which a small number of suppliers control the vast majority of supply of a product. Supply chain risks take many other forms, including geographic concentration, geopolitical, price and market volatility, environmental health and safety (EHS), intellectual property (IP), standards, substitution, integrity (counterfeits), and cybersecurity. Different technologies face different supply chain risks: information communications technology supply chains focus on cybersecurity risk. Conversely, raw materials supply chains focus much less on cybersecurity risk and far more on EHS risks associated with mining.

Characterizing critical technology supply chain risks is a sequential effort.[9] First, a technology's criticality must be assessed. Second, the supply chain of critical technologies must be mapped. These maps generally share similar segments regardless of the technology: raw materials are mined, refined, and processed into subcomponents, which are then incorporated into components that are then combined to form a finished system. Once these finished systems reach end of life (EOL), recycling and recovery is undertaken to generate raw materials for re-use.[10] Third, current vendors and alternate vendors are identified for each of these segments. Fourth, threats, vulnerabilities, and risks presented by the vendors are analyzed. Fifth, a determination to accept, reject, transfer, share, or mitigate these risks is made. Finally, an ongoing monitoring and assessment function re-evaluates each of these sequential steps over time.

2. China's Role in Critical Technology Supply Chains

Chinese firms maintain monopolies or near monopolies in many critical technology supply chain segments. Recent reports published by the U.S. government describe this dominance in detail both qualitatively and quantitatively.[11] In this section I present a quantitative open-source replicable methodology that uses international trade statistics to characterize U.S. import dependence on China

[8] https://www.usgs.gov/news/national-news-release/us-geological-survey-releases-2022-list-critical-minerals
[9] This section is derived from NIST SP 800-161 Rev. 1
[10] There are also important vendors adjacent to these segments, such as suppliers of specialty equipment or cybersecurity services.
[11] https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf

for critical technologies. Building on these findings, I describe a more qualitative example of the challenges imposed by China's dominance, the mitigation options for policymakers, and trade-offs.

2.1. Quantifying U.S. Critical Technology Industry Import Reliance on China

In 2018, the Congress passed the Foreign Investment Risk Review and Modernization Act, which resulted in the expansion of the Committee on Foreign Investment in the United States' mandate to review transactions of certain critical technology industries.[12] In response to this law, the Department of the Treasury identified 27 industries involved in critical technologies and their corresponding North American Industrial Classification System (NAICS) codes.[13] These industries included aircraft manufacturing, semiconductor manufacturing, batteries, and power distribution/transformers, among others. The NAICS codes are correlated with international trade statistics, making determination of aggregate imports and exports associated with a specific industry relatively straight-forward.[14]

Using the NAICS codes of technology industries defined as "critical" under the Department of the Treasury's pilot program, it is possible to determine U.S. imports from China for each of these industries and U.S. imports from the world for each of these industries. Analysis of U.S. imports from China as a percent of U.S. imports from the world for the time period between 2017-2021, showed U.S. reliance on imports from China of goods affiliated with these critical technology industries declined from 40% in 2017 to 36% in 2021. Not surprisingly, U.S. import dependence is particularly acute for information communication technologies and comparatively minor for aircraft and petrochemicals where the U.S. has a strong domestic supplier base. Additional details are presented in Appendix B.

The NAICS code analysis shows that ***China is responsible for over 1/3rd of U.S. imports of critical technology goods.*** However, U.S. import dependence on China for critical technology goods is even more pronounced when looking at specific critical technology industries and interpreting trade statistics more carefully. According to this NAICS code analysis, 40% of U.S. imports of storage batteries in 2021 were from China alone. Correlating this NAICS code with Harmonized Tariff System codes, which allow for more granular interpretation of trade data, shows that U.S. import reliance on China is more pronounced. For example, U.S. imports of lithium-ion batteries (HTS 8507.60) from China grew from $1 billion in 2017 (43% of total U.S. imports) to $4.2 billion in 2021 (56% of total U.S. imports).[15] Additional details are presented in Appendix C.

2.2. Qualitative Assessment of U.S. Battery Supply Chain on Imports from China

Lithium-ion batteries have been recognized in U.S. Department of Energy (DOE) and U.S. Department of Defense (DOD) supply chain reports as an important technology for economic and national security, making the import reliance on China described in the previous section a vulnerability.[16] However, the quantitative analysis presented in the previous section understates U.S. reliance on China for battery

[12] https://www.congress.gov/bill/115th-congress/house-bill/5841/text
[13] https://home.treasury.gov/system/files/291/Pilot-Program-FAQs.pdf
[14] All statistics derived from U.S. International Trade Commission (USITC) DataWeb: https://dataweb.usitc.gov/. There are several caveats to this analysis: (1) there are many critical technology industries that do not have a NAICS code (all software industries, for example); (2) several NAICS codes identified by Treasury do not have any trade affiliated with them (221113, 332117, 336414, 541713, 541714).
[15] All statistics derived from USITC DataWeb: https://dataweb.usitc.gov/.
[16] https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF; https://www.energy.gov/sites/default/files/2022-02/Energy%20Storage%20Supply%20Chain%20Report%20-%20final.pdf

technology. When the battery supply chain is broken down into segments, the acute dependence of the U.S. on China becomes apparent.

Raw Materials → Processed Materials → Subcomponents → Manufacturing → Recycling

The U.S. Geological Survey recently found that China was the leading producer of 16 out of 32 critical minerals identified in its 2022 report.[17] This leading position is particularly true for lithium-ion battery based materials. Lithium-ion batteries rely on cobalt, iron, nickel (C1), manganese, lithium, and graphite. China leads the world in raw material mining of graphite, accounting for 82% of the global production. The DOE recently found "China has near absolute dominance of today's refining capacity for metals necessary for lithium-ion batteries,"[18] which includes cobalt sulfate (62%), high-purity manganese sulfate (95%), and lithium hydroxide carbonate (61%). Similarly, for subcomponents, China's has dominance in the worldwide production of cathodes (63%), anode materials (84%), separators (66%), and electrolytes (69%). Finally, China leads in actual battery cell manufacturing (80%) and is expected to lead the market for recycling of these batteries (50%) as well. Importantly, forecasts show that China's share in each of these supply chain segments is expected to increase as under-development capacity comes online.[19]

The U.S. is attempting to mitigate some of these vulnerabilities, but mitigation efforts frequently come with trade-offs. The U.S. has abundant raw material resources, but increasing domestic mining and refining capacity has long lead times and well understood environmental trade-offs. One recent DOE report found that establishing mining and refining can cost up to $1 billion depending on mine depth, ore type, planned base material production, and location. Location factors include labor costs, taxes, land rents, and availability of infrastructure (water, energy, and transportation), making barriers to entry high.[20] These factors also implicate USG agencies with regulatory equities outside of the traditional supply chain world including the Environmental Protection Agency, the Department of the Interior, and the Army Corp of Engineers.

U.S. firms attempting to enter the subcomponent and product markets for lithium-ion batteries must also contend with high barriers to entry, unknown paths to commercialization, large established competitors, and price volatility. The DOD report noted that defense-specific custom design standards, acquisition policy, and a paucity of good industry data all compound the aforementioned vulnerabilities.[21] In response to these challenges, the DOD recently leveraged Defense Production Act Title III authorities to support development of critical materials for large-capacity batteries.[22] Other DOE-led ongoing initiatives in this domain include the Critical Minerals Institute, the Minerals Sustainability

---

[17] https://www.usgs.gov/news/national-news-release/us-geological-survey-releases-2022-list-critical-minerals
[18] https://www.energy.gov/sites/default/files/2022-02/Energy%20Storage%20Supply%20Chain%20Report%20-%20final.pdf (page nos.: 17-21)
[19] https://www.energy.gov/sites/default/files/2022-02/Energy%20Storage%20Supply%20Chain%20Report%20-%20final.pdf (page nos.: 17-21)
[20] https://www.energy.gov/sites/default/files/2022-02/PGM%20catalyst%20supply%20chain%20report%20-%20final%20draft%202.25.22.pdf (page no.: 13).
[21] https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF (page no.: 20)
[22] https://www.defense.gov/News/Releases/Release/Article/2989973/defense-production-act-title-iii-presidential-determination-for-critical-materi/

program, and Federal Consortium for Advanced Batteries.[23] Later in my testimony I will describe how these efforts could be coordinated to facilitate win-win investments across multiple critical technology supply chain segments.

3. U.S. Government Efforts to Review Supply Chains

In response to these challenges and others, the U.S. government (USG) has undertaken a wide variety of initiatives to review and manage critical technology supply chains.

The most recent and visible example of USG efforts to review supply chain security are the February 2022 reports prepared by the Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, and Homeland Security in response to Executive Order 14017 on America's Supply Chains.[24] These reports, which included both 100-day and 1-year deliverables, reviewed a wide variety of critical technology supply chains in industries important to U.S. economic and national security.[25]

The U.S. government has engaged in several supply chain review efforts in the past five years. These efforts include Executive Order 13817 and Executive Order 13953, both of which focused on increasing critical mineral supply chain security.[26] Relatedly, Executive Order 13806 tasked the DOD with analysis of its defense industrial base and supply chain resilience.[27] The Department of Commerce's Bureau of Industry and Security also maintains an industrial base assessments division which has published several reports on specific critical technologies and their supply chains in the past five years.[28] Moreover, the Government Accountability Office (GAO) regularly reviews government efforts to assess and manage supply chain risks, especially as they relate to critical technology. Recent GAO reports in 2020 and 2021 focused on government information technology supply chain risks and DOD efforts to protect critical technologies respectively.[29]

Several agencies maintain ongoing efforts to review supply chain vulnerabilities across sectors. The U.S. Geological Survey releases an annual "List of Critical Minerals" deemed important to "national security, [the] economy, renewable energy development and infrastructure."[30] The National Institute of Standards and Technology (NIST) at the Department of Commerce has produced SCRM guidelines for cybersecurity management designed to increase public and private sector supply chain resilience.[31] NIST is also currently studying the feasibility, advisability, and costs of establishing a national supply chain

---

[23] https://www.energy.gov/policy/articles/americas-strategy-secure-supply-chain-robust-clean-energy-transition (page no.: 23)

[24] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/

[25] https://www.whitehouse.gov/briefing-room/statements-releases/2022/02/24/the-biden-harris-plan-to-revitalize-american-manufacturing-and-secure-critical-supply-chains-in-2022/

[26] https://www.federalregister.gov/documents/2017/12/26/2017-27899/a-federal-strategy-to-ensure-secure-and-reliable-supplies-of-critical-minerals; https://www.federalregister.gov/documents/2020/10/05/2020-22064/addressing-the-threat-to-the-domestic-supply-chain-from-reliance-on-critical-minerals-from-foreign

[27] https://www.federalregister.gov/documents/2017/07/26/2017-15860/assessing-and-strengthening-the-manufacturing-and-defense-industrial-base-and-supply-chain.

[28] https://www.bis.doc.gov/index.php/other-areas/office-of-technology-evaluation-ote/industrial-base-assessments

[29] https://www.gao.gov/products/gao-21-171; https://www.gao.gov/assets/gao-21-158.pdf

[30] https://www.usgs.gov/news/national-news-release/us-geological-survey-releases-2022-list-critical-minerals

[31] https://www.nist.gov/news-events/news/2022/05/nist-updates-cybersecurity-guidance-supply-chain-risk-management

database.[32] The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has had a standing Information and Communications Technology (ICT) Supply Chain Management Task Force since December 2018.[33] The Department of Commerce is also leading the U.S. government's engagement with the European Union under the aegis of the U.S.-EU Trade and Technology Council to review critical technology supply chains and identify areas of collaboration to increase resilience.[34] Finally, the DOD produces an annual Industrial Capabilities report which presents the Department's priority industrial base risks and vulnerabilities within its supply chains.[35]

4. USG Efforts to Manage Supply Chains

The U.S. government's efforts to manage supply chain vulnerabilities are less expansive than the aforementioned efforts to review supply chains, and the maturity of these efforts varies by agency due to statutory authorities and scope of work. The reason for this divergence is simple: some agencies have sprawling supply chains and authorities, while others do not. For example, the F-35 Joint Strike Fighter relies on a supply chain of at least 1,900 companies and that system is just one of dozens of aircrafts that support DOD missions.[36] As a result of this vast industrial base, the DOD has entire sub-agencies dedicated to supply chain management and logistics (e.g., the Defense Logistics Agency)[37] as well as unique statutory authorities such as Title III of the Defense Production Act which provides for the use government funds to sustain critical production, commercialize research and development investments, and scale emerging technologies.[38] Conversely, the Department of Education has a much smaller supply chain and its statutory authorities related to supply chains are commensurately limited.

In general, the U.S. government manages supply chain vulnerabilities through four avenues: (1) identification and mapping of critical technology supply chains; (2) SCRM best practices; (3) applying SCRM standards to public sector operations; and (4) strategic allocation of funds to increase supply chain resilience through innovation, stockpiling, or financial aid to distressed but critical firms.

4.1. Mapping Critical Technology Supply Chains

The aforementioned government reports map critical technology supply chains with various levels of granularity and fidelity. These mapping efforts focus on determining specific supply chain segments and, in some cases, specific vendors and their market shares in these segments. Some of these mapping efforts are limited by a lack of access to data (which may be paywalled or simply not exist) or an inability to define the supply chain for a particular technology, which may be too nascent or emerging to have well-defined supply chain segments. In general, the supply chain vulnerabilities these reports identify are not systematically monitored or updated as supply chains change, but rather present a "snapshot in time" view. Harmonizing the varied methodologies used to map supply chains, data sources consulted, and the ad hoc nature of the risks identified and mitigation recommended would improve U.S. government efforts to review and manage supply chains across different agencies.

---

[32] https://www.nist.gov/document/chart
[33] https://www.cisa.gov/ict-scrm-task-force
[34] https://www.commerce.gov/news/press-releases/2022/05/us-eu-joint-statement-trade-and-technology-council
[35] https://www.defense.gov/News/Releases/Release/Article/2472854/dod-releases-industrial-capabilities-report/
[36] https://www.lockheedmartin.com/en-us/products/f-35/f-35-global-partnership.html#:~:text=Six%20Foreign%20Military%20Sales%20customers,nation%20acquiring%20the%20F%2D35
[37] https://www.dla.mil/AboutDLA/
[38] https://www.businessdefense.gov/ai/dpat3/overview.html.

4.2. Supply Chain Risk Management Best Practices

Various U.S. government agencies create "best practices" or standards documents designed to be shared with the public and private sector to harmonize SCRM efforts. NIST published Supply Chain Risk Management Practices for Federal Information Systems and Organizations in 2015 (updated as of May 2022) to provide guidance on identifying, assessing, and responding to cybersecurity risks throughout the supply chain at all levels of an organization."[39] CISA's ICT SCRM Task Force hosts an annual supply chain integrity month, has generated an SCRM toolkit, and maintains an ICT Supply Chain Resource Library.[40] In addition, the National Counterintelligence and Security Center (NCSC) hosts an annual "Supply Chain Integrity" month that includes a calendar of training events as well as a website with a repository of SCRM best practices documents generated by the public sector.[41] This summary of efforts is indicative, not exhaustive, and many of the subject matter specific resources contain best practices that are relevant across critical technology sectors.

4.3. Applying SCRM Standards to Public Sector Operations

The DOD and the intelligence community maintain a series of instructions and directives designed to promote SCRM best practices throughout their organizations. Department of Defense Instruction (DoDI) 4140.01 states the Department's supply chain material management policy while DoDI 5200.44 and 8500.01 focus on methods to establish trust and resilience in mission critical systems and cybersecurity.[42] Intelligence Community Directive (ICD) 731 was established in 2013 to protect the supply chain for mission critical products, materials, and services used across the intelligence community's organizations.[43] Subsequent directives have focused on supply chain criticality assessments, threat assessments, information sharing, vulnerability assessments, and risk assessments.[44] The Committee on National Security Systems has also issued a directive on SCRM.[45]

4.4. Strategic Allocation of Public Sector Funds

The U.S. government manages supply chains and mitigates known supply chain vulnerabilities through the use of funds to increase innovation, supports stockpiling, and provides financial support to particularly important suppliers. The DOE's Loan Programs Office (LPO) and Advanced Research Projects Agency–Energy (ARPA-E) distribute funds that can target sectors or technologies to increase innovation and resolve particular supply chain chokepoints.[46] Similarly, the Defense Advanced Research Projects Agency (DARPA) has funded initiatives focused on increasing semiconductor supply chain resilience as well as software development to provide real-time supply chain system awareness.[47] The Small Business Administration oversees the Small Business Innovation Research (SBIR) & Small Business Technology Transfer (STTR) program which provides federal funds to small innovative businesses to demonstrate

---

[39] https://www.nist.gov/news-events/news/2022/05/nist-updates-cybersecurity-guidance-supply-chain-risk-management

[40] https://www.cisa.gov/ict-scrm-task-force

[41] https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats.

[42] https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/414001p.pdf; https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf; https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/850001_2014.pdf

[43] https://www.dni.gov/files/NCSC/documents/supplychain/20190327-ICD731-Supply-Chain-Risk-Manage20131207.pdf

[44] https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats

[45] https://www.dni.gov/files/NCSC/documents/supplychain/CNSSD_505_Final2-891B85C3-.pdf

[46] https://www.energy.gov/lpo/loan-programs-office; https://arpa-e.energy.gov/

[47] https://www.darpa.mil/news-events/2020-05-27; https://www.darpa.mil/program/logx

project feasibility, develop prototypes, and commercialize promising technologies. The Defense Logistics Agency maintains the National Defense Stockpile, which stores 42 commodities ranging from zinc, cobalt, and chromium to platinum, palladium, and iridium, cumulatively valued at $1.1 billion.[48] The DOE's National Nuclear Security Administration also maintains a stockpile to support of the nuclear weapons enterprise.[49] Finally, the DOD's Industrial Base Policy office maintains the ability to conduct assessments of supply chains and distribute funds to firms engaged in the production of technologies that support national security under Title III of the Defense Production Act and the Cornerstone Other Transaction Authority (OTA), among others.[50]

5. USG Critical Technology Supply Chain Security: Harmonizing Definitions, Mapping, Risks, and Mitigation

The ultimate goal of U.S. critical technology supply chain security policies should be to ensure that for each segment of a critical technology supply chain there are at least three manufacturers located domestically or in allied countries that in combination have the capabilities to meet 50% of current and forecast domestic demands.[51] Where this goal is not attainable, the U.S. should have a process for determining if this supply chain risk should be accepted, rejected, transferred, shared, or mitigated.

Achieving this goal would restructure critical technology supply chains to increase their resilience and trust-ability. The goal of a comprehensive U.S. government supply chain security strategy should be establishment of a sustained capability aligned across executive branch agencies to:

- Develop a process to identify (and de-identify) a technology as "critical".
- Map, monitor, and assess technology supply chains deemed "critical".
- Create a qualitative and quantitative technology-agnostic supply chain risk assessment metric.
- Determine risk mitigation options and their trade-offs.
- Identify win-win investments that increase resilience across multiple supply chains shared by executive branch agencies.

There is a unique opportunity to increase harmonization of the aforementioned efforts to review and manage critical technology supply chains across agencies. U.S. government efforts to review and manage critical technology supply chains could be improved by: (1) harmonizing definitions of "supply chain" and "critical technology," (2) creating a template for interagency use when mapping critical technology supply chains, (3) developing a technology-agnostic supply chain risk assessment metric to determine vulnerabilities; (4) developing a taxonomy of supply chain risks; and (5) developing a register of mitigation options that corresponds with supply chain risks.

5.1. Shared Definitions of Supply Chain and Critical Technology

There are a wide variety of U.S. government definitions of "supply chain" and "supply chain risk management."[52] For example, the DOD, the Office of the Director of National Intelligence, and the National Institute of Standards and Technology at the Department of Commerce have all published

[48] https://www.dla.mil/Strategic-Materials/About/Our-Offices/
[49] https://www.energy.gov/nnsa/articles/stockpile-stewardship-and-management-plan-ssmp
[50] https://www.businessdefense.gov/ai/index.html
[51] These notional statistics are borrowed from: https://www.energy.gov/sites/default/files/2022-02/Electric%20Grid%20Supply%20Chain%20Report%20-%20Final.pdf (page no.: 44).
[52] See Appendix A for an indicative list drawn from NIST, DOD, and ODNI publications.

definitions of "supply chain" and "supply chain risk management." Harmonizing these definitions would support efforts to map supply chains by defining the key elements and actors. Harmonizing each of these agency's definitions of SCRM would likewise ensure that SCRM efforts are more aligned across the executive branch.

The U.S. government also has several different lists of "critical" and/or "emerging" technologies. The process of identifying critical technologies and developing a shared nomenclature to describe them is ongoing. Lists have been generated by the Department of Commerce's Bureau of Industry and Security (2018),[53] the White House (2020, 2022),[54] the Office of the Director of National Intelligence (2021),[55] the Department of Defense (2022),[56] and through the interagency coordinated effort in response to EO 14017.[57] These lists all make reference to advanced computing, artificial intelligence/machine learning, biotechnology, semiconductor technology, and quantum information science. Several lists are more expansive and also include technologies important to the financial industry (ex. distributed ledger technologies) and the energy sector industrial base (e.g., nuclear energy, fuel cells, batteries). A full comparison is provided in Appendix F.

Developing a harmonized list of critical technologies would help prioritize which supply chains to map, which threats and risks are short-term vs. long-term, and what mitigation options are available. Several U.S. government supply chain reports have presented examples of how to identify critical technologies and map their supply chains. For example, the DOE's supply chain reports used 10 criteria when considering whether a technology might be considered "critical":[58]

- **National security**: Is the technology critical to national security?
- **Exposure to supply chain risks**: Is the technology subject to supply chain risks stemming from limited domestic production and/or limited availability of raw materials, or malicious risks from foreign adversaries?
- **Importance to other critical infrastructure**: Are other critical infrastructure and energy systems reliant on the technology in a way that would compound supply chain vulnerabilities?
- **High-quality jobs**: Is there a significant opportunity to create sustained new high-quality jobs?
- **Decarbonization**: Is the technology a big contributor (e.g., new capacity additions) to U.S. decarbonization pathways? Can it reduce emissions by a certain target through Federal deployment?
- **Leverage of U.S. capabilities**: Could the manufacturing process leverage existing processes/capabilities where U.S. has technical leadership or a cost advantage, or where U.S. has ongoing research investments?

---

[53] https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies

[54] https://nps.edu/web/slamr/-/2020-national-strategy-for-critical-emerging-technologies; https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf

[55] https://www.dni.gov/index.php/ncsc-newsroom/item/2254-ncsc-fact-sheet-protecting-critical-and-emerging-u-s-technologies-from-foreign-threats

[56] https://www.cto.mil/usdre-strat-vision-critical-tech-areas/

[57] https://www.whitehouse.gov/briefing-room/statements-releases/2022/02/24/the-biden-harris-plan-to-revitalize-american-manufacturing-and-secure-critical-supply-chains-in-2022/.

[58] https://www.energy.gov/policy/articles/americas-strategy-secure-supply-chain-robust-clean-energy-transition (page no: 57)

- **Stage of commercialization**: Is domestic manufacturing near cost-competitive today or projected to be within five years given sufficient R&D or U.S. industrial policy?
- **Market size**: Is the projected global market for the technology big enough to support supply contributions from multiple economies? Is domestic demand alone sufficient to support a significant level of domestic manufacturing?
- **Global trade potential**: Is the supply chain for the technology subject to high shipping costs or other barriers that support domestic production (e.g., wind blades)?
- **Value add**: Does increased domestic production provide a significant increase in value added to the U.S. economy in comparison to existing manufacturing footprint?

5.2. Harmonizing Supply Chain Mapping Elements

Efforts undertaken by executive branch agencies in response to EO 14017 generated original and authoritative supply chain maps for many critical technologies. These efforts should serve as a template that subsequent USG supply chain mapping efforts can emulate. Importantly, these efforts produced model supply chain analyses of both high-technology readiness level (TRL)[59] (mature, existing) technologies as well as low-TRL (emerging) technologies. An example of this mapping is presented in Appendix E. Building on this mapping system for determining vendors for each raw material, subcomponent, component, and device will also feed in to the risk assessment described in the next section.

The supply chains of high-TRL existing and mature technologies all resemble the same general steps described above: raw materials are mined and refined, these refined materials are processed, the materials are then incorporated into subcomponents and components/systems, applied to their end use, and (ideally) recycled at EOL. In general, for mature supply chains, there are multiple suppliers in multiple countries capable of meeting the demand in each segment. Mapping should identify vendors for each segment of a critical technology supply chain as well as their market share and capacity.

The supply chains of emerging technologies with a low-TRL are necessarily harder to characterize and define. In emerging technology supply chains there may be cases wherein all segments are executed in-house by a vertically integrated firm or a well-defined vendor base for certain supply chain segments simply may not exist. Careful analysis of academic publications, patent filings, and technical standards as well as collaborations with industry and industry associations can help the government generate an indicative bill of materials (BOM) to define the steps in a particular emerging technology supply chain.

5.3. Technology-Agnostic Supply Chain Risk Assessment

Many of the supply chain analyses produced in response to EO 14017 demonstrated qualitative and quantitative supply chain risk assessments that could, and should, serve as a model for technology-agnostic risk assessments going forward.[60] A technology-agnostic supply chain risk assessment would consist of a set of criteria that could be used to assess existing and future threats, risks, and vulnerabilities regardless of the critical technology supply chain in question. Qualitative supply chain risk assessments are necessary when data on a particular industry is unreliable or unavailable. Quantitative supply chain risk assessments are ideal, but can only be accomplished when a variety of high fidelity data on the industry in question is available. For each critical technology supply chain segment, a

[59] https://api.army.mil/e2/c/downloads/404585.pdf.

[60] https://www.energy.gov/sites/default/files/2022-02/Nuclear%20Energy%20Supply%20Chain%20Report%20-%20Final.pdf (page no.: 51)

qualitative or quantitative assessment could be undertaken to characterize threats, vulnerabilities, and risks. For a particular critical technology sector, a model supply chain risk assessment[61] would determine:

- **Domestic supply and demand**: quantifying the number of domestic suppliers, their current capacity, and their ability to meet current domestic demand. Depending on data availability, supplemental research on domestic capacity under development and its ability to meet forecast demand would also be optimal.
- **Global supply and demand**: quantifying the number of international suppliers, the number that are located in friendly vs. adversary countries, and their respective abilities to meet current and projected global demand.
- **Net import reliance**: the dependence of a country on imports to meet domestic consumption, measured by the share of total apparent consumption that is provided by imports.
- **Market concentration:** the extent to which an industry or supply chain is controlled by a small number of firms or countries. Highly concentrated industries are those where a single or few factor(s) affect market outcomes, such as by restricting supply to raise prices, or by oversupplying the market to lower prices below a profitable level for competitors. The Herfindahl-Hirschman Index (HHI) is commonly used to quantify market concentration.[62]
- **Geopolitical sensitivity:** the strength of a producing nations' relationships with the U.S., covering issues including political stability, strength of institutions, labor rights issues, political rivalry, acrimonious relationship, and stability of supply coming from a given country.
- **Price and market volatility:** fluctuations in the price and supply/demand balance of a commodity. High volatility increases the cost and riskiness of doing business, as low prices may disincentivize new investments or make production unprofitable for producers, while high prices may make producers operating on the margin unprofitable. Price volatility is a particular issue in some raw materials markets.
- **Substitutability:** the ability of firms/supply chains to alter their material, product, manufacturing, or consumption patterns in response to price changes or other market shocks.
- **Environmental compliance and workplace safety conditions**: potential environmental damage and occupational safety and health practices that could result in unsteady supply. Producers that have a poor record of adherence to environmental policies have a greater likelihood of being shut down or penalized with fees (increasing costs), and those with poor safety records may face labor shortages or boycotts.
- **Barriers to entry:** large IP moats, standards ecosystems that result in control by one or more firms, and high startup costs all may impede the ability of a supply chain to innovate around chokepoints.
- **Competing application demand:** multiple industries may compete for the same product or upstream raw material, meaning supply of a particular product could become constrained due to a demand shock in an adjacent industry.
- **Lead time and qualification time:** the amount of time it takes to identify new suppliers, take delivery after an order has been purchased, and qualify the new product or service after delivery all impacts the resilience of a supply chain.

---

[61] https://www.energy.gov/sites/default/files/2022-02/PGM%20catalyst%20supply%20chain%20report%20-%20final%20draft%202.25.22.pdf (Page no.: 25) and https://www.energy.gov/sites/default/files/2022-02/Electric%20Grid%20Supply%20Chain%20Report%20-%20Final.pdf (Page no.: 43)

[62] https://www.justice.gov/atr/herfindahl-hirschman-index.

- **Technology readiness level:** an assessment to determine the TRL of the critical technology in question will assist in mapping the supply chain.
- **Stockpiling:** understanding what if any reserves are held in stockpiles and their sufficiency to meet current or forecast demand in the event of a supply shock.
- **End of life/recycling:** to what extent are recycled products an important feedstock to meet demand in a particular technology supply chain and under what circumstances might this supply change over time.

5.4. Taxonomy of Supply Chain Risks

There are a wide variety of supply chain risks. Depending on the critical technology supply chain, these risks include vendor concentration (single- or sole- source suppliers), geographic concentration (in a particular region), critical infrastructure failures, natural disasters, financial solvency of key vendors, IP theft, product tampering, cybersecurity, regulatory barriers, counterfeiting, workforce, substitutability (or lack thereof), geopolitics, and expropriation. Characterizing these risks in a systematic way is an important part of determining both the severity of the risk and identifying the mitigation options available.

Developing a shared taxonomy of risks that is applicable across supply chains would help the U.S. government better characterize the types of shared risks critical technology supply chains face, and identify the mitigation options available, and determine if any trade-offs exist. Some of the most comprehensive work by the U.S. government on this subject was done by U.S. Department of Homeland Security/CISA's ICT SCRM Threat Evaluation Working Group.[63] This group generated a list of supplier threats, categorized these threats, developed scenarios for threats, and reviewed and documented these scenarios specifically with reference to ICT supply chains.[64] These categories of risk included counterfeit parts, cybersecurity, internal controls, insider threat, economic, extended supply chain, legal, and end-to-end/external supply chain risks. This group also assigned "impact" and "likelihood" scores to each risk, the result of which generated a "risk score." Finally, this group also developed mitigation strategies which took in to account the estimated costs/trade-offs of implementing these mitigating strategies, how they would change likelihood/impact, and estimated residual risk. While specific to ICT supply chains, these efforts could serve as a model that other critical technology SCRM efforts may emulate.

5.5. Mitigation and Trade-offs

Once supply chain risks have been identified, impact and likelihood can be assigned to calculate an overall risk score. For the highest scoring risks, mitigation should be pursued. These risks can either be accepted, rejected, transferred, shared, or mitigated.[65] Each of these choices come with trade-offs, and understanding these trade-offs should be systematized so that policymakers clearly understand their options. A sample of the mitigation options identified by the DOE[66] is provided below:

- Increase domestic raw material availability.
- Expand domestic manufacturing capabilities.

[63] https://www.cisa.gov/ict-scrm-task-force.
[64] https://www.cisa.gov/ict-supply-chain-library
[65] https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final
[66] https://www.energy.gov/policy/articles/americas-strategy-secure-supply-chain-robust-clean-energy-transition

- Invest and support the formation of diverse and reliable foreign supply chains to meet global climate ambitions.
- Increase the adoption and deployment of clean energy.
- Improve EOL waste management.
- Attract and support a skilled U.S. workforce for the clean energy transition.
- Augment supply chain knowledge and decision-making.

However, more granular work could be done to define these mitigation options, their trade-offs, and next steps. For example, efforts to increase domestic raw material availability would require expansion of domestic mining. However, domestic mining can present environmental, health, and safety concerns which need to be weighed in to balance with the desire for greater supply chain security. In addition, mining regulations are overseen by agencies like the Department of the Interior and Environmental Protection Agency, that are not normally thought of as having major supply chain equities. Other supply chain risks have more difficult trade-offs.

Increasing domestic production of neodymium-iron-boron magnets (hereafter referred to as "rare-earth magnets") illustrates the complex mitigation and tradeoff options policymakers face. Rare-earth magnets are intensively used in generators, wind turbines, as well as national security systems,[67] making an increase in domestic production beneficial for multiple critical technology supply chains. The production of rare-earth magnets in the U.S. production has traditionally been limited across all segments of this supply chain, with China accounting for 58% of mining, 89% of separation, 90% of metal refining, and 92% of metal alloy manufacturing.[68]

Significant expansion of domestic U.S. offshore wind energy would create a commercial demand signal that may increase domestic production of these magnets.[69] However, increasing offshore wind energy production requires that the physical components used in wind turbines be delivered to their final destination and the size of these components is "approaching or over road and rail size limits, meaning the number of routes components can be transported from ports or factories to deployment is decreasing over time."[70] Even where overland transportation is an option, regulatory coordination with county, local, and state regulators is necessary. One alternative is delivering these components by sea, but doing so requires Jones Act-compliant maritime vessels.[71] And the "business case for [Jones Act-compliant maritime vessels] is challenged by lack of certainty in near-term offshore wind demand." As, this example shows, SCRM mitigation comes with complicated trade offs, some of which require regulatory harmonization and USG intervention beyond the discrete risk identified.

---

[67] https://www.energy.gov/sites/default/files/2022-02/Neodymium%20Magnets%20Supply%20Chain%20Report%20-%20Final.pdf (page no.: viii); https://www.federalregister.gov/documents/2021/09/27/2021-20903/notice-of-request-for-public-comments-on-section-232-national-security-investigation-of-imports-of.

[68] https://www.energy.gov/sites/default/files/2022-02/Neodymium%20Magnets%20Supply%20Chain%20Report%20-%20Final.pdf (page no.: 26)

[69] https://www.energy.gov/sites/default/files/2022-02/Neodymium%20Magnets%20Supply%20Chain%20Report%20-%20Final.pdf (page no.: viii); https://www.federalregister.gov/documents/2021/09/27/2021-20903/notice-of-request-for-public-comments-on-section-232-national-security-investigation-of-imports-of

[70] https://www.energy.gov/policy/articles/americas-strategy-secure-supply-chain-robust-clean-energy-transition (page no.: 17).

[71] https://www.energy.gov/policy/articles/americas-strategy-secure-supply-chain-robust-clean-energy-transition (page no.: 18)

5.6. Identifying Win-Win Supply Chain Investments to Support Critical Technologies

This section synthesizes the findings and recommendations in each of the preceding sections and presents an example of a critical technology supply chain strategy policymakers could consider. It recommends that policymakers look for investments that leverage shared market demand across critical technology supply chains. Specifically, it proposes that an increase in U.S. refining of copper would increase resilience in the semiconductor, battery, and pharmaceutical supply chains.[72]

Based on the findings presented earlier in this report, the lithium-ion battery supply chain is deemed critical by both the DOE and DOD for economic and national security reasons. However, mapping of this supply chain that was undertaken in response to EO 14017 found that most segments are located in China. More specifically, this mapping determined that U.S. domestic supply is insufficient to meet current and forecast demand, global demand is expected to increase substantially, market concentration is high, U.S. net import reliance is high, substitutability is low, there are substantial barriers to entry, several raw materials face competing application demand, and that EOL/recycling is a growth area but the U.S. is not currently positioned to take full advantage of this growth.

Policymakers should pay particular attention to critical technology supply chains where competing application demand is identified as a risk. This risk can be mitigated and turned in to an opportunity that actually increases critical technology supply chain resilience. For example, in the case of battery supply chains, copper was identified as low risk raw material in recent U.S. government reports given that "The United States mines, smelts, refines, and recycles copper, and it has significant copper reserves..."[73]

In spite of this seemingly stable supply chain, increased domestic copper refining capacity would have favorable subsequent effects for the semiconductor and pharmaceutical industries as well the battery industry. Even though the U.S. mines and refines some copper, refined copper accounted for 85% of all unmanufactured copper imports in 2021.[74] Refined copper is particularly important for several technology industries in addition to batteries. The semiconductor industry primarily relies on refined copper for "back-end" assembly, test, and packaging. Specifically, copper is one of many materials used to connect a manufactured chip to a PCBs. In response to a recent Commerce Department Request for Information, one industry representative stated "the domestic electronics industrial base is lacking additive process capability to produce ultra-fine copper circuits."[75] A recent report from the DOE on the semiconductor supply chain identified direct bond copper (DBC) insulator substrates as a particular chokepoint.[76] The pharmaceutical industry also increasingly relies on copper catalyst, a byproduct of copper refining, as a substitute for harder-to-source materials used in drug synthesis.[77] Both industries are expected to intensively consume these copper refining byproducts in the future. Finally, several U.S. companies make equipment that uses copper, among many other materials, to serve the semiconductor and battery markets.[78] Increasing copper refining capacity in the U.S. would increase the resilience of these supply chains as well.

---

[72] For this example I am grateful to my PNNL colleague Dr. Mark Willey.

[73] https://www.energy.gov/sites/default/files/2022-02/Fuel%20Cells%20%26%20Electrolyzers%20Supply%20Chain%20Report%20-%20Final.pdf (page no.: 31)

[74] https://pubs.er.usgs.gov/publication/mcs2022

[75] https://www.regulations.gov/comment/BIS-2021-0011-0090

[76] https://www.energy.gov/sites/default/files/2022-02/Semiconductor%20Supply%20Chain%20Report%20-%20Final.pdf (page no.:5)

[77] https://onlinelibrary.wiley.com/doi/abs/10.1002/anie.201609837

[78] https://arpa-e.energy.gov/technologies/projects/new-electrode-manufacturing-process-equipment

6. Conclusion

U.S. efforts to review and manage critical technology supply chains are ongoing and require greater interagency coordination to realize their potential. Additional supply chain efforts should incorporate existing best practices across the government. These best practices[79] include:

- Mapping critical technology supply chains by segment, by vendor (including their market share and capacity)
- Identifying existing and future threats, risks, and vulnerabilities.
- Identifying opportunities and major barriers; including financial and commercial, scientific, technical, regulatory, and market barriers.
- Identifying areas where government and private sector can collaborate to expand the industrial base for multiple USG agencies
- Identifying specific actions needed to incentivize companies in critical technology sectors to re-shore or near-shore manufacturing investments
- Identifying specific actions to address threats, risks, and vulnerabilities and help build resilient supply chains.

The goal of U.S. critical technology supply chain security policies should be to ensure that for each segment of a critical technology supply chain there are at least three manufacturers domestically or in friendly countries that combined are able to meet 50% of current and forecast domestic demand.

To summarize several of the points made earlier in my testimony, there are several considerations that should be taken in to account if the U.S. government wants to increase critical technology supply chain resilience:

- **Interagency coordination and harmonization of supply chain initiatives**:
    - Harmonize definitions, directives, mapping, and best practices: The Intelligence Community, the Department of Defense, and the National Institute of Standards and Technology have developed a series of directives, instructions, and best practices related to supply chains and supply chain risk management. This work should be increasingly coordinated by these, and other, executive branch agencies. Examples of productive collaborations could include developing:
        - Shared definitions of “supply chain” and “SCRM”
        - Shared best practices for mapping supply chains
        - Shared best practices reflected in DOD instructions and Intelligence Community Directives on supply chains and SCRM
    - Increase interagency participation in supply chain work: In addition to agencies with obvious supply chain equities such as the Departments of Defense and Energy, The U.S. Geological Survey, the U.S. International Trade Commission, and the Environmental Protection Agency all have important roles to play in mapping supply chains, characterizing chokepoints/U.S. import dependence, and determining the viability of

[79] https://www.energy.gov/policy/articles/americas-strategy-secure-supply-chain-robust-clean-energy-transition (page no.: 3).

mitigation (ex. identifying regulatory hurdles to domestic mining production expansion) respectively. Increasing their participation in ongoing SCRM efforts would be valuable.
    - For example, using it's access to high fidelity trade data, the U.S. International Trade Commission could undertake a Section 332 Fact Finding Investigation to determine U.S. Net Import Dependence on Critical Technologies, using the methodology introduced in Section 2 of my written testimony.
- **Leverage critical technology supply chain co-dependencies**: Building upon the efforts undertaken in response to EO 14017, executive branch agencies could integrate their findings to identify critical technology supply chains and supply chain segments that share co-dependencies and/or competing application demand
    - For example, reports by the Department of Energy and Department of Defense noted that large castings and forgings are important for some renewable energy generation, nuclear energy, and shipbuilding and there is a dearth of U.S. availability.
    - Using existing statutory authorities under the DPA and DOE LPO, among others, these agencies could coordinate increased and prioritized funding for critical technology supply chains and supply chain segments that result in win-win resiliency outcomes for raw materials, sub-component, and component manufacturing in the U.S. and allied countries.
- **Coordinate information collection and dissemination**: Sustained critical technology supply chain information collection, integration, monitoring, and analysis is also necessary as technology supply chains evolve, vendors enter or exit a market, and USG systems increase or reduce their reliance on a technology.
    - This information sharing could take the form of a new supply chain office or standing interagency committee that leverages access to relevant USG data sources and private sector information providers to conduct ongoing SCRM assessments and identifies win-win mitigation opportunities.

Appendix A. U.S. Government Definitions of Supply Chain and Supply Chain Risk Management

Agency	Supply Chain	Supply Chain Risk Management (SCRM)
DOD[80]	"The linked activities associated with providing material to end users for consumption. Those activities include supply activities (such as organic and commercial ICPs and retail supply activities), maintenance activities (such as organic and commercial depot level maintenance facilities and intermediate repair activities), and distribution activities (such as distribution depots and other storage locations, container consolidation points, ports of embarkation and debarkation, and ground, air, and ocean transporters)."	"The process for managing risk by identifying, assessing, and mitigating threats, vulnerabilities, and disruptions to the DOD supply chain from beginning to end to ensure mission effectiveness."
NIST[81]	"[A] linked set of resources and processes between and among multiple levels of organizations, each of which is an acquirer, that begins with the sourcing of products and services and extends through their life cycle."	"A systematic process for managing exposure to...risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures."
ODNI[82]	"A supply chain is a network of people, processes, technology, information, and resources that delivers a product or service. Key supply chains are essential to protecting critical infrastructure; countering economic exploitation; and defending against cyber and technical operations."	"The management of risk to the integrity, trustworthiness, and authenticity of products and services within the supply chain."

[80] https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/414001p.pdf
[81] https://doi.org/10.6028/NIST.SP.800-161r1
[82] Office of the Director of National Intelligence (ODNI); https://www.dni.gov/files/NCSC/documents/supplychain/20200925-NCSC-Supply-Chain-Risk-Management-tri-fold.pdf; https://www.dni.gov/files/documents/ICD/ICD%20731%20-%20Supply%20Chain%20Risk%20Management.pdf

Appendix B. China as a Percent of U.S. Imports for Select Critical Technologies, 2017-21[83]

NAICS Code	Description	2017	2018	2019	2020	2021
325110	Petrochemicals	1%	1%	0%	0%	0%
325180	All other basic inorganic chemicals	11%	12%	8%	7%	7%
331313	Alumina refined and primary aluminum	0%	0%	1%	0%	0%
331314	Secondary smelting & alloying of aluminum	13%	9%	7%	0%	0%
332991	Ball & roller bearings	21%	21%	20%	20%	20%
333242	Semiconductor machinery	34%	32%	15%	18%	15%
333314	Optical instruments &lenses	25%	24%	22%	24%	24%
333611	Turbines & turbine generator sets	19%	14%	11%	12%	4%
334111	Electronic computers	66%	61%	55%	58%	61%
334112	Computer storage devices	22%	13%	4%	3%	1%
334210	Telephone apparatus	75%	73%	65%	48%	57%
334220	Radio/TV broadcast & wireless communication equip	63%	63%	61%	56%	55%
334413	Semiconductors & related devices	11%	11%	6%	5%	5%
334511	Search, detection & navigation instruments	10%	9%	5%	5%	6%
335311	Power/distribution/specialty transformers	10%	10%	7%	7%	5%
335911	Storage batteries	30%	33%	33%	32%	40%
335912	Primary batteries	39%	36%	33%	36%	32%
336411	Aircraft	0%	0%	0%	0%	0%
336412	Aircraft engines & engine parts	2%	2%	2%	2%	2%
336415	Missile/space vehicle propulsion units & parts	0%	0%	0%	0%	0%
336419	Missile/space vehicle parts & auxiliary equip.	1%	2%	2%	3%	3%
336992	Military armored vehicle, tank & tank components	0%	0%	0%	0%	0%
	Total	40%	39%	35%	36%	36%

[83] https://dataweb.usitc.gov/; There are several caveats to this analysis: (1) there are many critical technology industries that do not have a NAICS code (all software industries, for example); (2) several NAICS codes identified by Treasury do not have any trade affiliated with them in USITC data (221113, 332117, 336414, 541713, 541714).

Appendix C. China as a Percent of U.S. Imports of Storage Batteries[84]

NAICS Code	HTS Code	HTS Code Description	2017	2018	2019	2020	2021
335911: Storage Battery Manufacturing	8507.10.00	Lead-acid storage batteries of a kind used for starting piston engines	6%	6%	5%	6%	3%
	8507.20.40	Lead-acid storage batteries of a kind used as the primary source of electrical power for electrically powered vehicles of 8703.90	13%	60%	39%	37%	60%
	8507.20.80	Lead-acid storage batteries other than of a kind used for starting piston engines or as the primary source of power for electric vehicles	36%	35%	21%	16%	15%
	8507.30.40	Nickel-cadmium storage batteries, of a kind used as the primary source of electrical power for electrically powered vehicles of 8703.90	37%	48%	4%	4%	4%
	8507.30.80	Nickel-cadmium storage batteries, other than of a kind used as the primary source of power for electric vehicles	30%	22%	23%	20%	23%
	8507.40.40	Nickel-iron storage batteries, of a kind used as the primary source of electrical power for electrically powered vehicles of 8703.90	10%	15%	44%	64%	0%
	8507.40.80	Nickel-iron storage batteries, other than of a kind used as the primary source of power for electric vehicles	40%	19%	16%	13%	12%
	8507.50.00	Nickel-metal hydride batteries	35%	38%	34%	26%	14%
	8507.60.00	Lithium-ion batteries	43%	47%	51%	47%	56%
	8507.80.40	Other storage batteries, of a kind used as the primary source of electrical power for electrically powered vehicles of 8703.90	26%	16%	3%	4%	1%
	8507.80.81	Other storage batteries, other than of a kind used as the primary source of power for electric vehicles	56%	65%	24%	26%	35%
	8507.90.40	Parts of lead-acid storage batteries, including separators therefor	14%	10%	22%	39%	35%
	8507.90.80	Parts of storage batteries, including separators therefor, other than parts of lead-acid storage batteries	11%	9%	18%	17%	30%

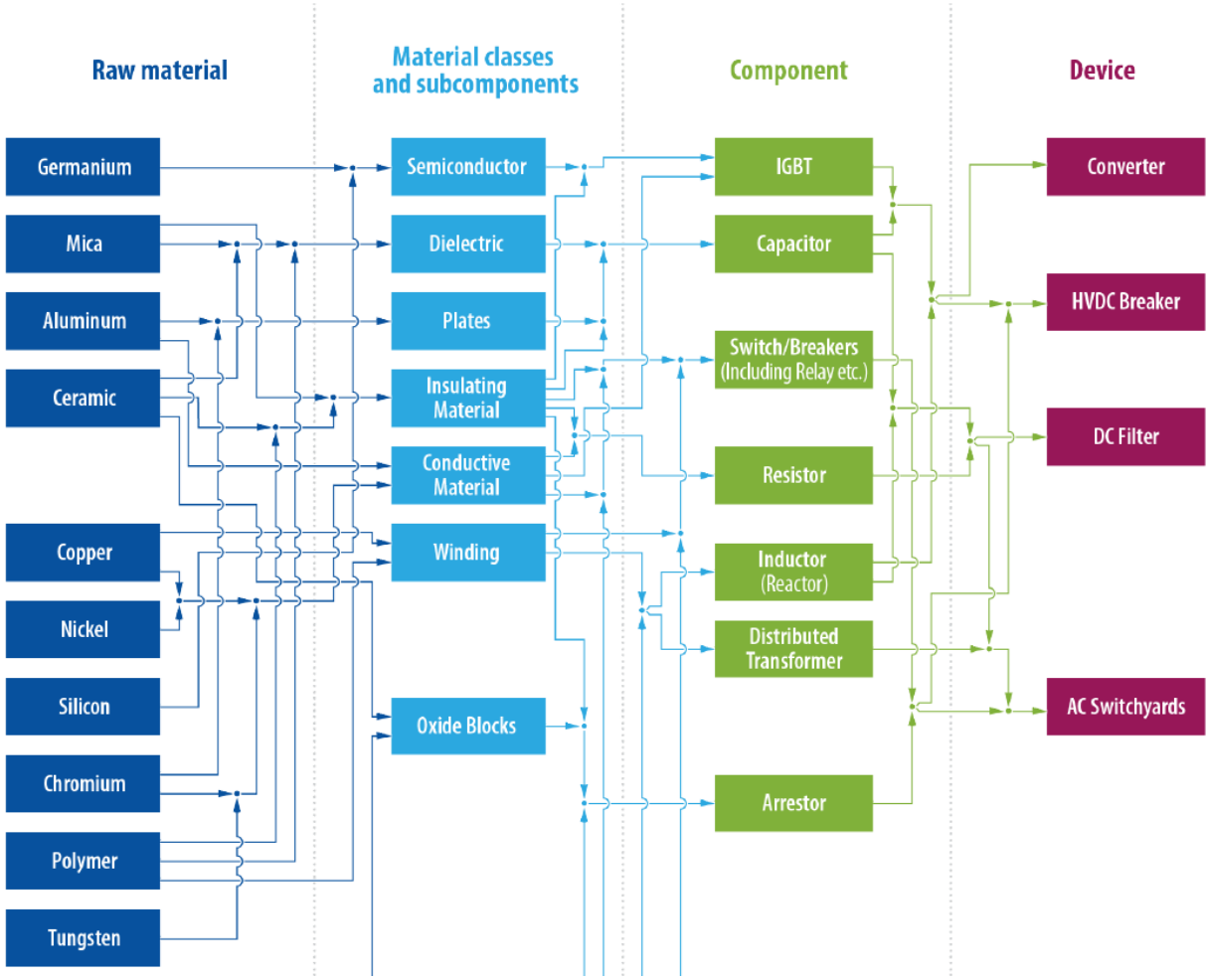
[84] https://dataweb.usitc.gov/; Data is presented in percentages, which may overstate the criticality of the import dependency as overall import values may be small.

Appendix D. Example Supply Chain Risk Factors[85]

Risk	Definition
Barriers to Entry	Is there a regulatory/IP moat that new entrant firms must overcome?
Complexity	Is technical know-how essential for realizing value?
Components	Are there components on which a product relies? <100? >100?
Concentration of Suppliers	Are any supply chain segments supplied by fewer than 3 vendors or does one vendor account for 50% of capacity?
Consolidation of Suppliers (Geographic)	Is more than 50% of worldwide capacity concentrated in one country?
Consumption	Is consistent, ongoing supply of the good, necessary (not a one off purchase)?
Durability	Is maintenance/servicing required for ongoing use?
Excellence	Is there a distinction between the capabilities of SOTA and non-SOTA?
Intensity of Consumption	Is the item a once per month, once per year, or once per decade purchase?
Inter-Industry Demand	Do other industries compete for the same product? (Could supply disappear for reasons exogenous to this industry?)
Inter-Industry Supply	Does the industry using it generate it? (Is supply of good tied to the industry that consumes it or exogenous?)
Intrinsic Value	Is the thing by itself worth anything to anyone else or is it industry-specific?
Lead Time	How long would it take to purchase and take delivery of a replacement under normal circumstances?
Location of Suppliers	Is a replacement available domestically?
Mobility	Are transport costs high?
National Security	Does the stand-alone product pose an obvious national security threat?
Political/Social Interest	Has the good or service been subject to recent export controls, environmental objections etc.?
Qualification Time	Does a user need to ensure a replacement inter-operates with existing process? If so, under what timeframe?
R&D Intensity	Is it complicated to produce (is R&D required for any replacement)?
Stockpiling	Is stockpiling an option? Would stockpiling result in obsolescence, half-life concerns etc.?
Substitutability	Are there ways to innovate around an observed supply chain segment chokepoint?
Technology Readiness Level	What is the TRL?
Value Added	How much value does it add to final product?
Zero Sum (Fixed Supply?)	If your competitor buys more of the product, does that mean there is less available for you?

[85] This list is derived in part from: https://www.energy.gov/sites/default/files/2022-02/Neodymium%20Magnets%20Supply%20Chain%20Report%20-%20Final.pdf (page no.: 23)

Appendix E. Example of Supply Chain Mapping[86]



[86] https://www.energy.gov/sites/default/files/2022-02/Electric%20Grid%20Supply%20Chain%20Report%20-%20Final.pdf

Appendix F. U.S. Government Critical Technology Lists[87]

Critical Technology Category	Commerce/BIS Emerging Technology List (2018)	WH Critical and Emerging Technologies List (2020)	ODNI (2021)	DOD Critical Technology Areas (2022)	WH Critical and Emerging Technologies List (2022)	EO 14017 Critical Supply Chain Reports: Sectors Covered (2022)
Advanced/Integrated Sensing, Signature Management, & Systems		X		X	X	
Advanced Computing	X	X		X	X	
Advanced Conventional Weapons Technologies		X				X
Advanced Engine Technologies		X			X	X
Advanced Materials + Advanced/Additive Manufacturing	X	X		X	X	X
Advanced Surveillance Technologies	X					
Agricultural Technologies		X				X
Artificial Intelligence/Machine Learning	X	X	X	X	X	
Autonomous Systems		X	X	X	X	
Biotechnologies	X	X	X	X	X	X
Chemical, Biological, Radiological, & Nuclear (CBRN) Mitigation Technologies		X				
Communication & Networking Technologies		X		X	X	X
Data Analytics Technology	X	X				
Directed Energy				X	X	
Renewable Energy Technologies		X		X	X	X
Financial/Distributed Ledger Technologies		X			X	
Human-Machine Interfaces	X	X			X	
Hypersonics	X		X	X	X	
Logistics Technology	X					X
Medical & Public Health Technologies		X				X
Nuclear Energy Technologies					X	X
Position, Navigation, & Timing (PNT) Technologies	X					
Quantum Information Science	X	X	X	X	X	
Robotics	X					
Semiconductors & Microelectronics	X	X	X	X	X	X
Space Technologies & Systems		X		X	X	

[87] Note that some technology names have been paraphrased to harmonize the nomenclature across lists. Sources include:
Commerce (2018): https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies;
WH (2020): https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-regarding-national-strategy-critical-emerging-technologies/;
ODNI (2021): https://www.dni.gov/index.php/ncsc-newsroom/item/2254-ncsc-fact-sheet-protecting-critical-and-emerging-u-s-technologies-from-foreign-threats;
DOD (2022): https://www.cto.mil/wp-content/uploads/2022/02/usdre_strategic_vision_critical_tech_areas.pdf;
WH (2022): https://www.whitehouse.gov/ostp/news-updates/2022/02/07/technologies-for-american-innovation-and-national-security/;
EO 14017 Reports (2022): https://www.whitehouse.gov/briefing-room/statements-releases/2022/02/24/the-biden-harris-plan-to-revitalize-american-manufacturing-and-secure-critical-supply-chains-in-2022/.