SHIELD
by SOURCEREE

What's Inside

National Security Newsletter

June 2021

SOURCEREE

In our June 2021 SHIELD Newsletter, we are doing a lookback at the results of some issues we've been tracking since day one. First up is the White House 100 day supply chain review report. The report outlined vulnerabilities to the supply chains in four sectors: semiconductors, high-capacity batteries, and rare earth elements (REEs) – industries Sourceree continues to monitor closely – in addition to health care and pharmaceuticals. Next is the prepared testimony of Government Accountability Office Director of Information Technology and Cybersecurity. Director Vijay A. D'Souza identifies current and past threats to the Information and Communications Technology (ICT) supply chain paired with a series of seven recommended actions and the report card for 23 federal agencies. Federal agencies who are out of compliance with those recommendations have identified lack of federal supply chain risk management (SCRM) guidance as the primary factor. Then we provide some key excerpts from the National Intelligence Council's outlook to the year 2040 and what state global power competition and industry readiness from ice caps to space might look like, and what we can do to be ready. We close with the Office of the Undersecretary of Defense for Acquisition and Sustainment's first Annual Report, released at the end of April 2021. They highlight their progress in 2020, including reviewing CFIUS cases; progressed Defense Trade Modernization; and performed due diligence and accepted over 100 members into the Trusted Capital Marketplace.

-- Adam Murphy, Sourceree President

Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth

The White House

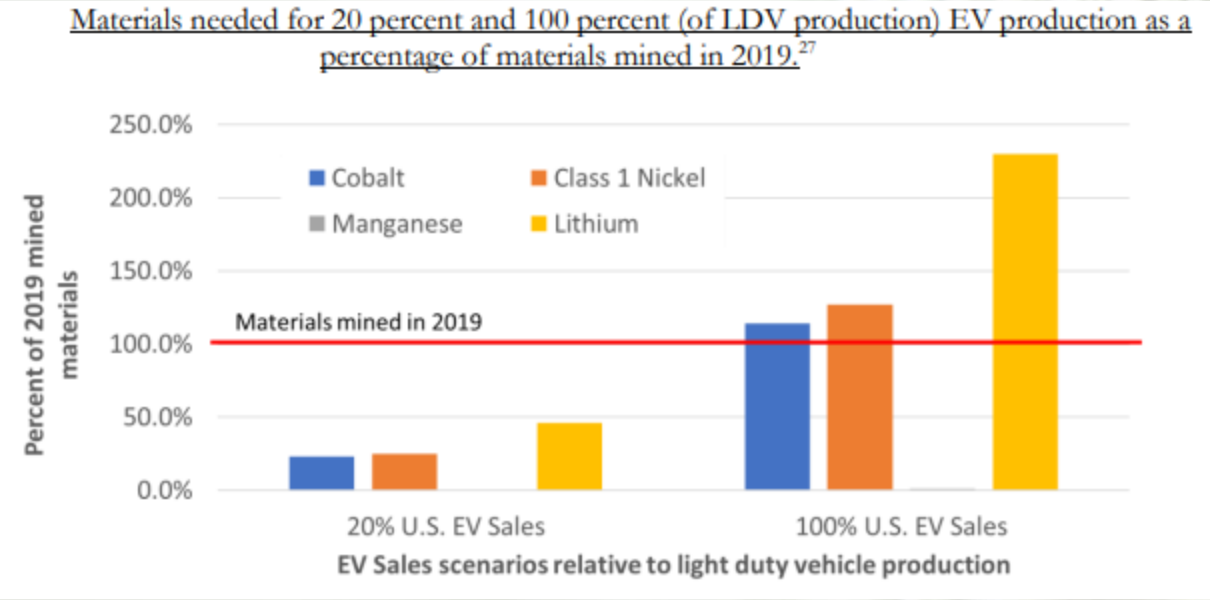
8 June 2021

100 days after President Biden signed EO 14017, the four Executive Branch departments responsible for a study on protecting America's supply chain released their final report. The full report digs deeper into semiconductors, rare earth elements (REEs), and high-capacity batteries along with the health and pharmaceutical supply chain, but consistently identifies domestic production in a globalized world as the solution.

Select excerpts from the piece:

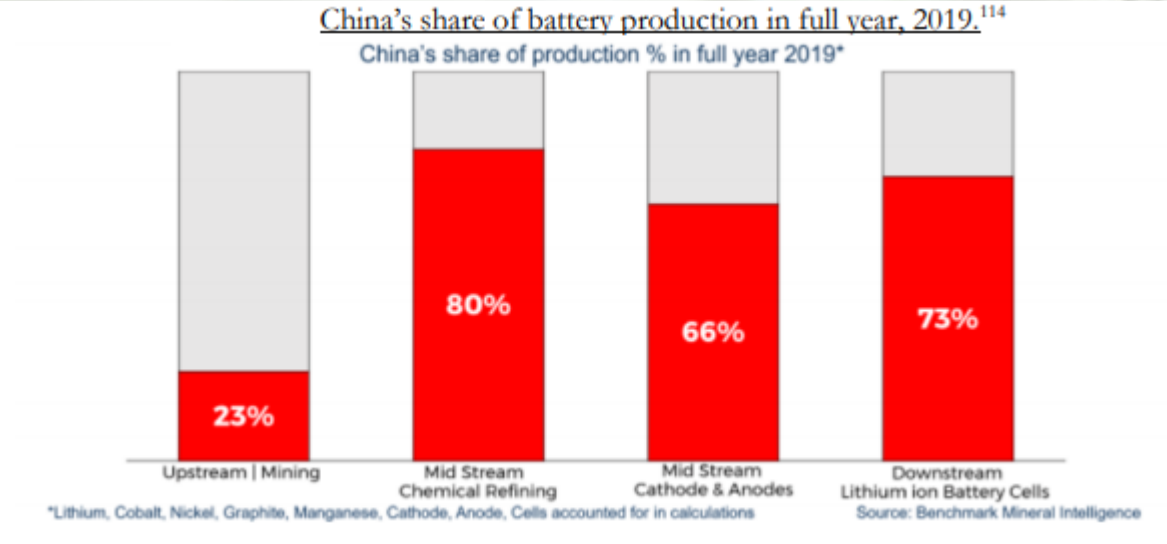
National security experts, including the Department of Defense, have consistently argued that the nation's underlying commercial industrial foundations are central to our security. Reports from both Republican and Democratic administrations have raised concerns about the defense industry's reliance on limited domestic suppliers; a global supply chain vulnerable to disruption; and competitor country suppliers. Innovations essential to military preparedness—like highly specialized lithium-ion batteries—require an ecosystem of innovation, skills, and production facilities that the United States currently lacks.

Our economic security—steady employment and smooth operations of critical industries—also requires secure and resilient supply chains. For more than a decade, the Department of Defense has consistently found that essential civilian industries would bear the preponderance of harm from a disruption of strategic and critical materials supply. The Department of Energy notes that, today, China refines 60 percent of the world's lithium and 80 percent of the world's cobalt, two core inputs to high-capacity batteries—which presents a critical vulnerability to the future of the U.S. domestic auto industry.



Drivers of Supply Chain Vulnerability

- **Insufficient U.S. manufacturing capacity;**
- **Misaligned Incentives and short-termism in private markets;**
- **Industrial Policies Adopted by Allied, Partner, and Competitor Nations;**
- **Geographic concentration in global sourcing:** To ensure resilient supply chains, it is essential that they be globalized. However, the search for low-cost production, combined with the effective industrial policy of key nations, has led to geographic concentrations of key supply chains in a few nations, increasing vulnerabilities for United States and global producers. Such concentration leaves companies vulnerable to disruption, whether caused by a natural disaster, a geopolitical event or indeed, a global pandemic. From the studies conducted pursuant to E.O. 14017, it is clear in the Department of Commerce's report that the United States is dangerously dependent on specific countries for parts of the value chain of all of these products. The global economy depends on Taiwanese firms for 92 percent of leading-edge semiconductor production. China has over 75 percent of global cell fabrication capacity for advanced batteries, as noted in the Department of Energy's report. While the Department of Health and Human Services' data suggests India and China compete for market share of many U.S. medicines, industry analysis suggests India imports nearly 70 percent of its APIs from China.
- **Limited International Coordination.**



Recommendations

1. Rebuild our production and innovation capabilities

Use immediate administrative authorities to support an ecosystem of producers and innovators including SMEs and skilled workers:

- **Work with industry and labor to create pathways to quality jobs, with a free and fair choice to join a union, through sector-based community college partnerships, apprenticeships and on-the-job training;**
- **Support small, medium and disadvantaged businesses in critical supply chains:** The Small Business Administration (SBA) should support the diversification of critical suppliers through a targeted effort to better coordinate SBA's range of investment and technical assistance programs for small businesses and disadvantaged firms in the four targeted industries and firms seeking to enter those industries. SBA lending and investment products provide vital capital to small businesses, and the Small Business Investment Company program offers long-term equity investment in critical competitiveness sectors. The Small Business Innovation Research and Small Business Technology Transfer competitive programs, will support a diverse portfolio of small businesses to meet research and development needs, and increase commercialization;
- **Examine the ability of the U.S. Export-Import Bank (EXIM) to use existing authorities to further support domestic manufacturing:** We recommend that EXIM develop a proposal for Board consideration regarding whether and how to implement a new Domestic Financing Program to support the establishment and/or expansion of U.S. manufacturing facilities and infrastructure projects in the United States that would support U.S. exports. The proposal would support and facilitate U.S. exports while rebuilding U.S. manufacturing capacity.

2. Support the development of markets that invest in workers, value sustainability, and drive quality

3. Leverage the government's role as a purchaser of and investor in critical goods. As a significant customer and investor, Federal Government has the capacity to shape the market for many critical products. The public sector can deploy this power in times of crisis—such as in the recent public-private partnerships to facilitate development and delivery of a COVID-19 vaccine—or in normal times. The Administration should leverage this role to strengthen supply chain resilience and support national priorities.

4. Strengthen international trade rules, including trade enforcement mechanisms. Establish a trade strike force: We recommend the establishment of a U.S. Trade Representative-led trade strike force to identify unfair foreign trade practices that have eroded U.S. critical supply chains and to recommend trade actions to address such practices. We also recommend that supply chain resilience be incorporated into the U.S. trade policy approach towards China. We also recommend that the trade strike force examine how existing U.S. trade agreements and future

trade agreements and measures can help strengthen the United States and collective supply chain resilience.

5. Work with allies and partners to decrease vulnerabilities in the global supply chains.

6. Monitor near term supply chain disruptions as the economy reopens from the COVID-19 pandemic.

- Establish a Supply Chain Disruptions Task Force: We recommend the Administration establish a new Supply Chain Disruptions Task Force that will provide an all-of-government response to address near-term supply chain challenges to the economic recovery. The Task Force will be led by the Secretaries of Commerce, Transportation, and Agriculture and will focus on areas where a mismatch between supply and demand has been noted over the past several months: homebuilding and construction, semiconductors, transportation, and agriculture and food. The Task Force will bring the full capacity of the federal government to address near-term supply/demand mismatches. It will convene stakeholders to diagnose problems and surface solutions—large and small, public or private—that could help alleviate bottlenecks and supply constraints.
- Create a data hub to monitor near term supply chain vulnerabilities: We recommend that the Commerce Department lead a coordinated effort to bring together data from across the federal government to improve the federal government's ability to track supply and demand 18 disruptions and improve information sharing between federal agencies and the private sector to more effectively identify near term risks and vulnerabilities.

Federal Agencies Need to Implement Recommendations to Manage Supply Chain Risks

Testimony before the Subcommittees on Investigations and Oversight and Research and Technology, Committee on Science, Space and Technology, House of Representatives
Vijay A. D'Souza, Director, Information Technology and Cybersecurity, Government Accountability Office (GAO)
25 May 2021

In testimony to the U.S. House of Representatives, the GAO Director for Information Technology and Cybersecurity identified a series of previous findings on vulnerabilities to the U.S. federal government's Information & Communications Technology (ICT) supply chain, recommendations, and agency compliance status and impact for 23 federal agencies. Among the industries and technologies noted as having supply chains vulnerable to cyber attack were pipelines, bulk energy, avionics, and 5G. Additionally, the GAO plans to release a detailed report evaluating federal agencies' response to SolarWinds in fall 2021.

Select excerpts from the testimony:

The exploitation of ICT products and services through the supply chain is an emerging threat. ICT supply chain-related threats can be introduced in the manufacturing, assembly, and distribution of hardware, software, and services. Moreover, these threats can appear at each phase of the system development life cycle, when an agency initiates, develops, implements, maintains, and disposes of an information system. As a result, the compromise of an agency's ICT supply chain can degrade the confidentiality, integrity, and availability of its critical and sensitive networks, IT-enabled equipment, and data.

Over the past several years, Congress and federal agencies have taken a number of steps aimed at mitigating ICT supply chain risks. Despite these measures, we have previously reported that federal agencies have not effectively managed supply chain risks.

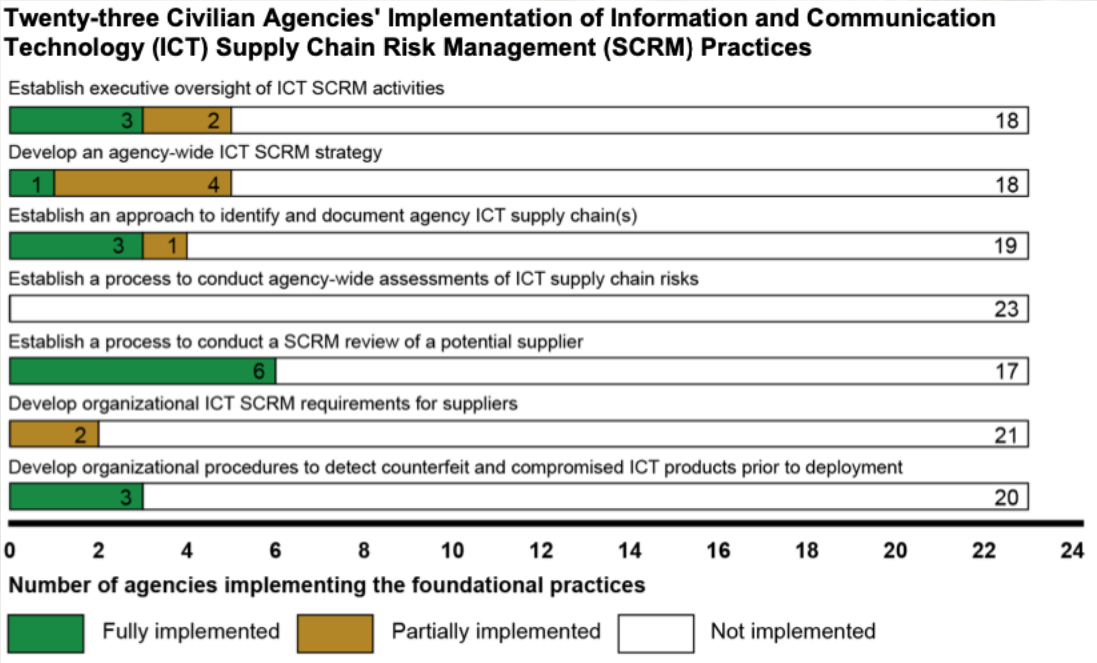
Few Federal Agencies Implemented Foundational Practices for Managing ICT Supply Chain Risks

The recent compromise of SolarWinds highlights the significance of threats to the ICT supply chain. In December 2020, we reported on the 23 civilian agencies' implementation of foundational practices for managing ICT supply chain risks. In that report, we identified and selected the seven practices from NIST's guidance that are considered foundational for an organization-wide approach to ICT SCRM. These selected foundational practices are:

- establishing executive oversight of ICT activities, including designating responsibility for leading agency-wide SCRM activities;
- developing an agency-wide ICT SCRM strategy for providing the organizational context in which risk-based decisions will be made;
- establishing an approach to identify and document agency ICT supply chain(s);
- establishing a process to conduct agency-wide assessments of ICT supply chain risks that identify, aggregate, and prioritize ICT supply chain risks that are present across the organization;

- establishing a process to conduct a SCRM review of a potential supplier that may include reviews of the processes used by suppliers to design, develop, test, implement, verify, deliver, and support ICT products and services;
- developing organizational ICT SCRM requirements for suppliers to ensure that suppliers are adequately addressing risks associated with ICT products and services; and
- developing organizational procedures to detect counterfeit and compromised ICT products prior to their deployment.

However, as we discussed in our report, none of the 23 agencies had fully implemented all of the supply chain risk management practices. Further, 14 of the 23 agencies had not implemented any of the practices. Figure 1 summarizes the extent of the agencies' implementation of the practices.



As a result of not fully implementing these selected foundational practices, the agencies are at a greater risk that malicious actors could exploit vulnerabilities in the ICT supply chain, causing disruptions to mission operations, harm to individuals, or theft of intellectual property. For example, without establishing executive oversight of SCRM activities, agencies are limited in their ability to make risk decisions across the organization about how to most effectively secure their ICT product and service supply chains. Moreover, agencies lack the ability to understand and manage risk and reduce the likelihood that adverse events will occur without reasonable visibility and traceability into supply chains.

Officials from the 23 agencies cited various factors that had limited their implementation of the selected foundational practices for managing supply chain risks. The most commonly cited factor was the lack of federal SCRM guidance.

Global Trends 2040: A More Contested World

National Intelligence Council
8 April 2021

Among the Key Takeaways of the Office of the Director on National Security's (ODNI) outlook on global stability in the year 2040 are an existential threat that transforms multilateral cooperation and disrupts economic incentives; a reshuffled geopolitical hierarchy that foresees a stronger partnership between Europe and the People's Republic of China; countries reliant on fossil fuels being the slowest to adapt to the changing landscape; and global priorities taking precedence over national interests. Using climate change as one of the persistent forces altering our current world order, ODNI presents five potential scenarios for 2040.

Select excerpts from the piece:

During the next two decades, several global economic trends, including rising national debt, a more complex and fragmented trading environment, a shift in trade, and new employment disruptions are likely to shape conditions within and between states. Many governments may find they have reduced flexibility as they navigate greater debt burdens, diverse trading rules, and a broader array of powerful state and corporate actors exerting influence.

During the next two decades, the pace and reach of technological developments are likely to increase ever faster, transforming a range of human experiences and capabilities while also creating new tensions and disruptions within and between societies, industries, and states. State and nonstate rivals will vie for leadership and dominance in science and technology with potentially cascading risks and implications for economic, military, and societal security.

Climate Change Contributes to Instability and Conflict Risk

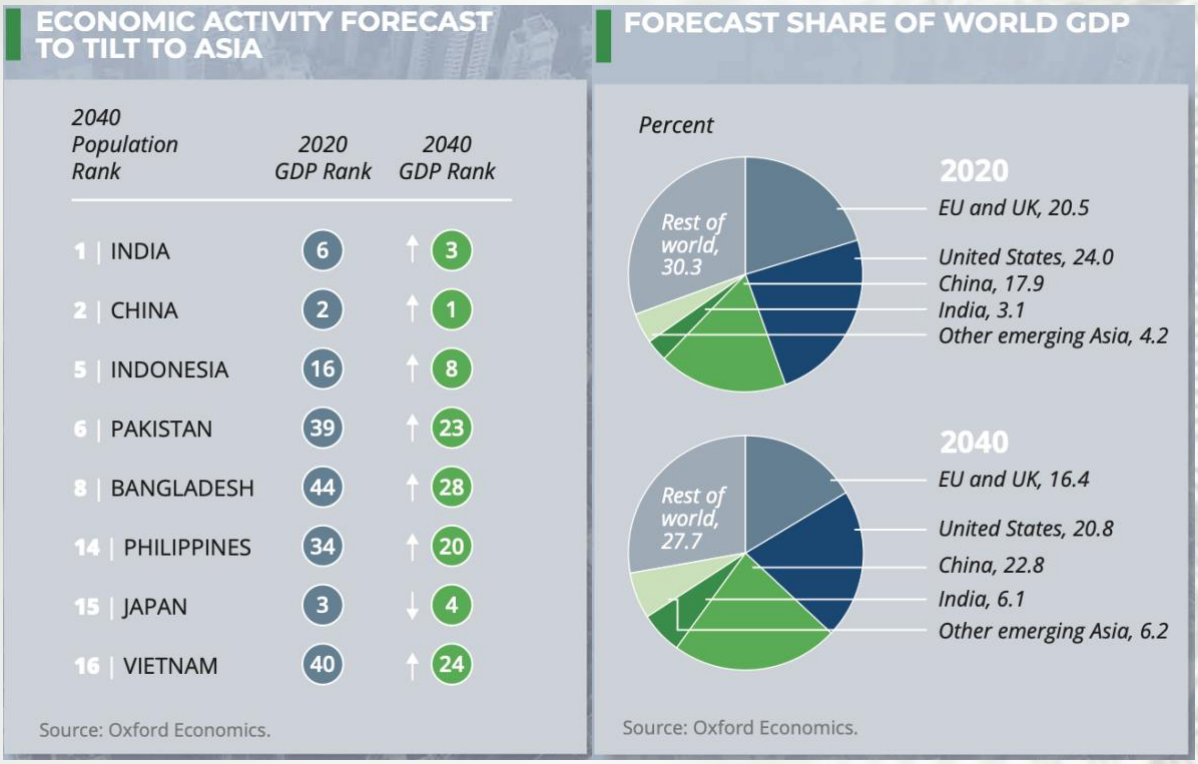
Rarely is climate change the sole or even primary driver of instability and conflict; however, certain socio-political and economic contexts are more vulnerable to climate sparks that ignite conflict. Countries of particular concern are those with ethnic or religious polarization; livelihoods highly dependent on natural resources or agriculture; weak or illegitimate conflict resolution mechanisms; a history of violence; and low adaptive capacity. For example, an increase in drought or extreme weather may reduce the opportunity cost of joining armed groups for struggling farmers and herders, while sectarian elites may advance their polarizing political goals by exploiting local grievances exacerbated by climate change.

Strains Military Readiness

While militaries will continue to adapt and fight in the changing world, climate effects will strain readiness and compound fiscal pressures on many militaries. Storm surges and sea level rise will force changes to the design and protection of naval bases and aircraft runways, prolonged extreme heat will limit training days, and major storms and floods will force militaries to divert more resources to disaster relief at home and abroad.

Multinational "Superstar" Firms Perpetuate Economic Globalization

State-owned multinationals (SOM - NCs), most of which originated in China, India, Russia, Saudi Arabia, United Arab Emirates (UAE), and some EU member countries, almost certainly will continue to be active participants in international commerce. Some SOMNCs may distort the global competitive landscape because of the state support that they receive. As the competition for technology leadership intensifies, SOMNCs, including those from China, could increase their reliance on state support to capture and lock-in first mover advantages, prompting private companies to lobby their governments to intervene on their behalf.



Growing Competition for Dominance

The race for technological dominance is inextricably intertwined with evolving geopolitics and is increasingly shaped by broader political, economic, and societal rivalries, particularly those associated with China's rise. Amassing the resources to sustain broad technology leadership, including the concentration of human talent, foundational knowledge, and supply chains, requires decades of long-term investment and visionary leadership. Those focusing their resources today are likely to be the technology leaders of 2040. In open economies, a mix of private efforts and partnerships between governments, private corporations, and research programs will compete with state-led economies, which may have an advantage in directing and concentrating resources, including data access, but may lack the benefits of more open, creative, and competitive environments.

Security and Privacy Reimagined

Current notions of privacy will continue to evolve, with individuals needing to share more personal information for access to applications, and tracking becoming ubiquitous. Authoritarian governments are likely to exploit increased data to monitor and even control their populations. Moreover, many companies and organizations will also have powerful tools such as video manipulation, or deep fakes, to improve tailored marketing or advance a particular narrative. Emerging AI applications may also become potential targets for data manipulation to skew their output.

China As A Space Power

By 2040, China will be the most significant rival to the United States in space, competing on commercial, civil, and military fronts. China will continue to pursue a path of space technology development independent of that involving the United States and Europe and will have its own set of foreign partners participating in Chinese-led space activities. Chinese space services, such as the Beidou satellite navigation system, will be in use around the world as an alternative to Western options.

Space Supporting Government and Military Needs

The space landscape in 2040 will combine emerging technology with a maturation of today's capabilities to help drive commercialization and introduce new applications. Services, such as communications, navigation, and satellite imagery, will become ubiquitous offering improved capabilities, lower costs, and increasing efficiencies. The efforts of both government and commercial actors will establish new domains of space competition, particularly between the United States and China.

Complicating Government-Corporate Relationships

Public-private partnerships for investment, research, and development have been critical for attaining many technological breakthroughs and advantages, but core corporate and national interests do not naturally align. Large technology companies increasingly have resources, reach, and influence that rivals and even surpasses some states. National interests in maintaining technological control and advantage as well as protecting national security can be at odds with corporate interests in expanding global market share and increasing profits.

Disrupting Industries and Jobs

The pace of technological change, notably developments in advanced manufacturing, AI, and biotechnology, may hasten disruptions to manufacturing and global supply chains, eliminating some modes of production and jobs and bringing supply chains closer to markets. Shifting supply chains could disproportionately affect less advanced economies, while many new jobs will require workers with improved or retooled skills.

Acquisition & Sustainment: 2020 Annual Report

Office of the Undersecretary of Defense for Acquisition and Sustainment
28 April 2021

In April 2021, the Department of Defense Office of Acquisition and Sustainment released its 2020 annual report to highlight its achievements in data and vignettes. Each accomplishment aligns with the framework of the U.S. National Defense Strategy, which has the following lines of effort: restore military readiness as we build a more lethal force; expand and strengthen alliances and partnerships; and bring business reform to the Department of Defense. In 2020, OUSD(A&S) achieved that across a spectrum of activities including small business support, cybersecurity, and CFIUS reviews.

Select excerpts from the piece:

This document aims to convey how A&S and the Department as a whole have successfully implemented the NDS over the last year and the measurable impact we have created, as illustrated by data and specific examples of our efforts over the last year.

OUSD(A&S) is proud to submit our inaugural annual historical record – the first of many. We believe that our efforts in 2020 have led to transformational changes for the Department, efforts we expect to have a long-lasting, positive impact for our Warfighters.

Industrial Policy – Ensuring robust, secure, resilient, and innovative industrial capabilities upon which DoD can rely in an era of great power competition to fulfill current and future Warfighter requirements

231 **CFIUS Case Reviews** As a member of the Committee on Foreign Investment in the United States, DoD, and specifically OUSD(A&S), review certain foreign acquisitions, mergers, or takeovers of U.S. businesses to determine the effect of a transaction on national security. While data for 2020 is still being finalized, in 2019, Industrial Policy processed 231 CFIUS cases on behalf of DoD.

Industrial Base Council

The IBC was reconstituted to pursue a DoD-wide approach to address shared Industrial base issues and vulnerabilities based on the risk framework outlines in Executive Order 13806, Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States. The IBC efforts align national defense priorities to ensure industrial base readiness and resiliency, and provide governance on resource and policy decisions from defense-wide industrial base risk mitigation strategies.

International Cooperation – Strengthening key international partnerships to improve interoperability and sharpen the Warfighter's technological edge

Defense Trade Modernization

In conjunction with OSD, ASD(A), and numerous industry stakeholders, IC completed 32 of 37 critical actions the Department can take internally to better align our conventional arms transfers with our national security interests. This Defense Trade Modernization (DTM) effort is addressing the dynamic tension between the necessity to protect our technological edge and the need to equip our partners and allies with cutting-edge capability. Its four areas of focus include:

- Exportability: Increasing the competiveness of U.S.-made systems by building exportability into design and development.
- Releasability: Updating DoD's technology release framework, including revising outdated policies and processes.
- Market Space/Interoperability: Working with partners and allies to identify critical capability requirements and expediting transfers that support these imperatives.
- Industrial Capacity: Incentivizing increased industrial production capacity to facilitate timely delivery of systems to our partners and allies.

Information and Cybersecurity – Innovating ways to measure and mitigate cyber risk to mission throughout the acquisition and sustainment lifecycle

Trusted Capital Marketplace

Launched in December, the Trusted Capital Marketplace has over 75 companies and 30 capital providers participating. Each has undergone a rigorous due diligence process before their acceptance into the marketplace to ensure foreign ownership, control, and influence was nonexistent. Trusted finance partners applied via the Trusted Capital landing page, and technology innovation providers all received a recommendation to the program after being selected by one of the Services through our rapid acquisition channels.

Protected by

SHIELD
by SOURCEREE

Sourceree's SHIELD program is a comprehensive supply chain risk management (SCRM) solution designed to help answer questions about supply chain disruptions and risks, particularly foreign investment.

SHIELD VISION

Software platform for on-demand supply chain risk assessments and financial intelligence

SHIELD SQUAD

Analytical Support

SHIELD INTEL

Business intelligence reports on critical suppliers