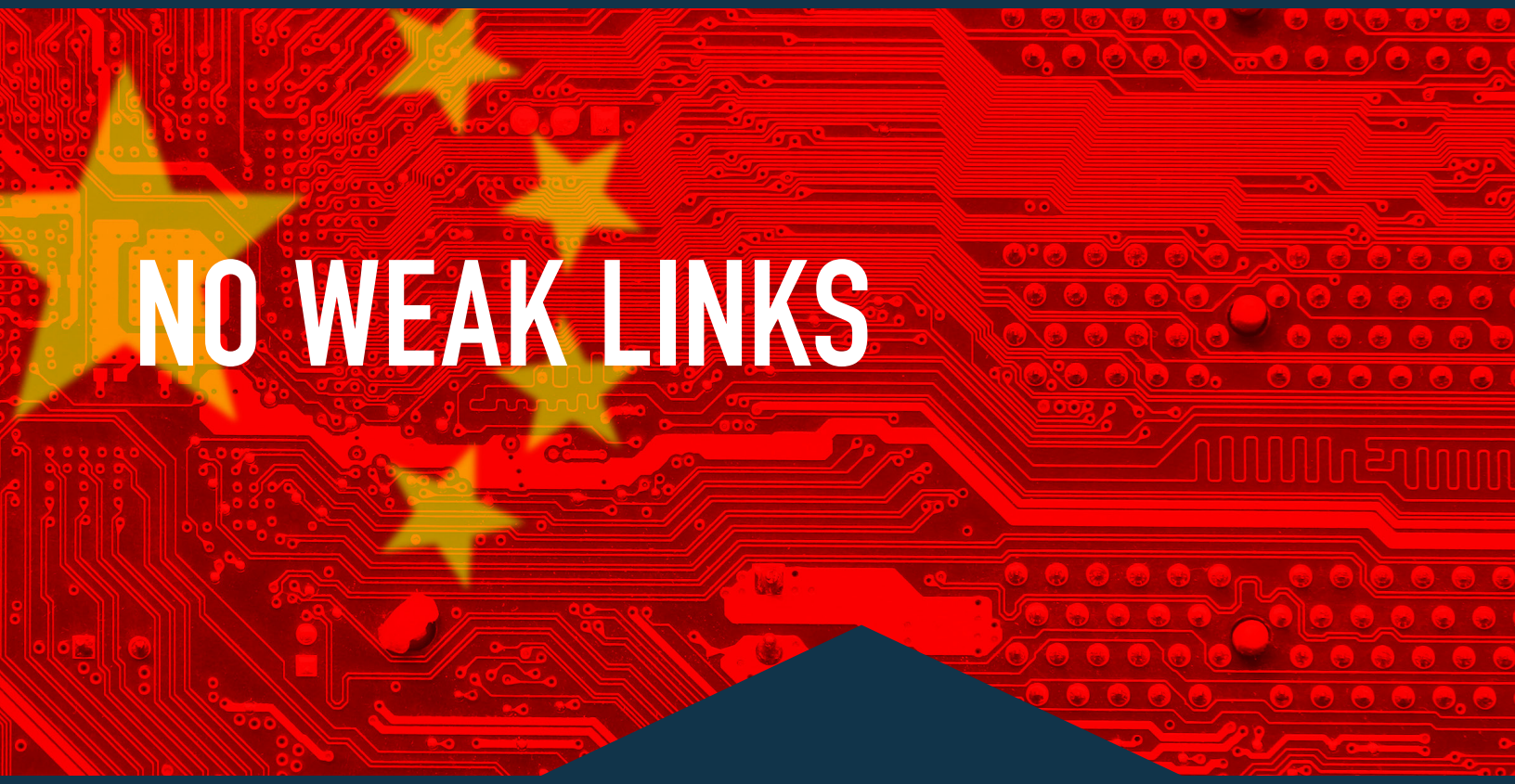


NO WEAK LINKS

A STRATEGY FOR KEEPING U.S. DEFENSE SUPPLY CHAINS CLEAN OF DANGEROUS CHINESE TECHNOLOGIES

JUNE 1, 2023

IN CONSULTATION WITH NAZAK NIKAKHTAR, CHINA TECH THREAT SPECIAL ADVISOR[1]

China TECH THREAT

TABLE OF CONTENTS

PREFACE: WHY THE U.S. GOVERNMENT NEEDS TO ENSURE "CLEAN" SUPPLY CHAINS FOR DOD AND OTHER AGENCIES

The United States Government controls troves of sensitive information. Agencies responsible for American defense, intelligence, and diplomatic efforts, as well as numerous other federal agencies, rely on billions of dollars' worth of technologies to protect that information. Keeping that information secure is always a challenge, as the recent case of alleged leaker Jack Teixeira, a Massachusetts Air National Guardsman, indicates. Foreign adversaries' attempts to penetrate U.S. systems can have equally or even more damaging consequences.

Unfortunately, major government contractors may unwittingly be compromising sensitive information in their reliance on on electronic technology and/or software manufactured by companies owned or controlled by foreign adversaries, especially China. Today many items used by the federal government – e.g. smartphones, batteries, vehicles, and weapons systems – contain components with backdoor surveillance capabilities that retrieve sensitive U.S. Government information, "kill switches" that enable a foreign adversary to disable equipment while in use or tamper with the device remotely, causing systems disruptions or intentional malfunction. The additional reality is that a substantial quantity of these foreign-sourced components come from the People's Republic of China (PRC).

FBI Director Christopher Wray says that there is "no country that presents a broader threat" than the People's Republic of China.[2] At the same time, China is both a major technology manufacturer and home to a 2017 intelligence law which compels Chinese companies and citizens to turn over to the Chinese government any information it deems necessary for national security purposes. While Chinese business leaders have said they would refuse government directives, independent analysts insist they would be forced to comply.

> "They have no position to say no to the Chinese government."[3]
>
> *- Dr. Miles Yu, former State Department China Policy Advisor, commenting on the obligations of Chinese companies under Chinese law*

So why would contractors rely on suspect technology and how could our adversaries use backdoors? In recent years, Chinese President Xi Jinping has directed tens of billions of dollars in investments into semiconductor national champions YMTC, SMIC, and CXMT, growing their market share by 30 percent.[4] These sizable investments, coupled with China's non-market economy structure where prices of goods, land, electricity, and labor are intentionally distorted by the central government, enable Chinese products to be priced lower than competitors by approximately 40%-60% in many instances. But these price discrepancies are artificial (not driven by market forces), and are always subject to manipulation by the Chinese government. Nevertheless, major American contractors working with the U.S. Government have opted over the past 15 years to rely on Chinese electronics equipment and software, largely because Chinese products are less expensive.

It is technologically conceivable that the Chinese government could tamper with certain products in ways that would put U.S. national security interests in serious peril.[5] One prominent weapons system used on Ukrainian battlefields is BAE Systems' AGM88 harm air-to-surface missile.[6] This weapon relies on an array of highly sophisticated semiconductors. What if it was built with semiconductors from PRC-controlled companies and the PRC manipulated the microchips to disable the weapons?

While there are a handful of U.S. Government procurement regulations that prohibit the acquisition of Chinese equipment, the regulations are not fully enforced. Government contractors also lack adequate visibility into their upstream supply chains to ensure their own compliance. The U.S. Government has itself acknowledged many times that it lacks full visibility into its own supply chain dependence on Chinese entities. This creates a serious vulnerability in both the security of its electronics communications systems and its military systems.

The U.S. government does not know the extent to which Chinese technologies have penetrated the defense supply chain. This lack of visibility can and should be cured, and the process of doing so is not prohibitively complex. The solution depends on (1) knowing which critical government systems may rely on insecure technology and (2) replacing the technology with items sourced from trusted suppliers.

PROBLEM STATEMENT: CONTRACTORS' OPAQUE SUPPLY CHAINS INVITE INFILTRATION

Present high-technology supply chains are extremely layered. Federal government vendors, contractors, and "primes" (original equipment manufacturers) often lack adequate visibility into the supply chains of their second tier, third tier, etc. suppliers of goods or software. This lack of visibility encourages supply chain infiltration by foreign adversaries. Such risk to U.S. Government systems is unacceptable: infiltration into the Government's information and communications technology and services ("ICTS") systems and defense systems can introduce surveillance and/or hardware malfunction capabilities that could compromise America's communications, intelligence, and weapons capabilities and put the Defense Department's warfighters in serious peril. These vulnerabilities could impact allies as well, to the extent they procure U.S. equipment and software, and vice versa.

The core problem with existing supply chain rules is that they require self-policing without any enforcement mechanism.

At present, some, albeit limited, U.S. Government authorities exist that discourage or outrightly prohibit reliance on materials sourced from certain Chinese entities. These include the Federal Acquisition Regulations, the Defense Federal Acquisition Regulations Supplement, the Consolidated Appropriations Act of 2018, Section 889 of the 2019 National Defense Authorization Act ("NDAA") and Section 5949 of the 2023 NDAA. The core problem with these rules is that they require contractors to self-police, which most (if not all) simply lack the will (but not the resources) to do.[7] Nor does the U.S. Government have a mechanism to enforce these prohibitions, which means that vendors routinely ignore these requirements. The risks associated with ignoring supply chain vulnerabilities are too great and the Government's mitigation strategy needs to evolve

SOLUTION: INFORMATION GATHERING AND U.S. GOVERNMENT REPORTING THROUGH DEFENSE PRODUCTION ACT SURVEYS

Despite U.S. Government inaction to date, the Government does have authority to compel vendors to review their supply chain vulnerabilities and report them to the Government. For example, the Pentagon can mandate its primes to audit their supply chains for risks. Pursuant to authorities under section 705 of the Defense Production Act of 1950 as amended ("DPA") (50 U.S.C. app. 2155) and § 104 of Executive Order 13603 of March 16, 2012 (National Defense Resources Preparedness, 77 FR 16651, 3 CFR, 2012 Comp., p. 225), the U.S. Government conducts studies to determine whether the U.S. industrial base's capabilities appropriately support the U.S. Government, defense sector, or the broader domestic commercial supply chain.

To produce these studies, the Government (through the Department of Commerce) may issue Defense Production Act Surveys to collect detailed information related to the health and competitiveness of the U.S. industrial base from Government sources and private individuals or organizations. Such surveys are mandatory (they operate analogous to subpoenas) and are routinely issued to assess specific weak links in supply chains. Unfortunately, to date, the Surveys have not been used to comprehensively probe the supply chains of vendors that provide critical ICTS and defense capabilities to the U.S. Government. This is a significant shortcoming. The U.S. government has the capabilities to identify the source of the technological components in its supply chains. It should use them.

SURVEY METHODOLOGY AND OUTPUT: The following describes how the U.S. Government, including the Pentagon, could compel contractors and defense primes to audit their supply chains. The end goal would be for these contractors/primes to (1) certify that the chains are clean from components/software sourced from entities associated with foreign countries of concern or (2) report to the Government the presence of problematic components/software in their supply chains. Entities associated with foreign countries of concern would be entities located in or affiliated with (through ultimate beneficial owners, "UBOs") foreign countries of concern (including but not limited to China and Russia) – hereinafter collectively referred to as Foreign Entities of Concern, i.e., "FEOCs." The audit steps are straightforward and could materially affect the U.S. Government's supply chains for the better.

The Commerce Department, which would administer the Surveys, would start with a pilot project that could then be replicated for the broader industrial base, as follows:

1. COMMERCE DEPARTMENT ISSUES SURVEYS TO CONTRACTORS

Commerce would develop and issue on behalf of federal agencies surveys to all U.S. Government contractors/primes within a specific sector, for example unmanned aerial systems. (UAS). The

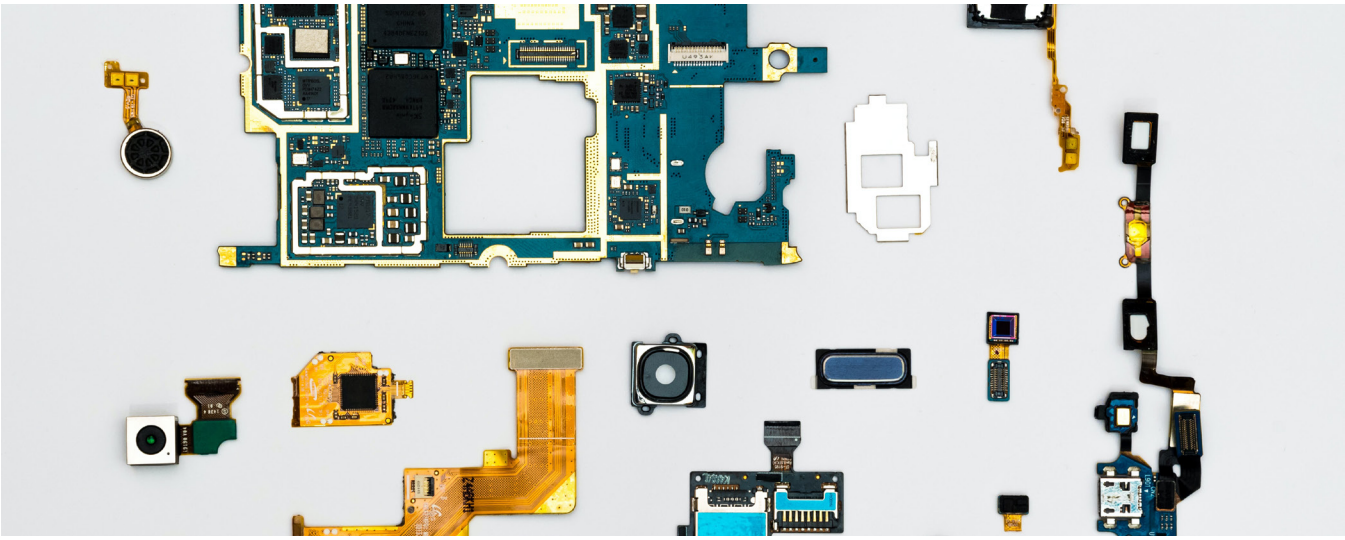
surveys would request information from the contractors/primes as to their material and software supply chains, and then require the contractors/primes to identify any potential critical components/software sourced from FEOCs. The following information would specifically be required:

a. All bills of materials ("BOMs") required to produce the final product (e.g., UAS) and imbedded critical components (e.g., lithium-ion batteries).

b. All software bills of materials ("SBOMs") required to produce the imbedded software.[8]

c. Description of all critical components/software included in the BOMs/SBOMs sourced from FEOCs. Critical components/software are all parts of the final product that could be used by a foreign adversary to (1) damage the operations of the final product, (2) create safety risks, (3) collect and transmit surveillance-type data from or through the final product or any related component/software, and (4) cause any other harm to U.S. national security.

d. Certification from the contractor/prime that it has conducted a complete audit of its supply chains up to the critical components/software, and that it confirms the absence of critical components/software from FEOCs, or if such supply chain vulnerabilities exist such that a certification cannot be provided, the contractor/prime would be required to report the supply chain vulnerability to the U.S. Government.



2. SURVEY RECIPIENTS CONDUCT DUE DILIGENCE

Upon receipt of the surveys, contractors/primes would need to take the following steps to comply with requirements 1.a-d:

a. Obtain the requested BOMs and SBOMs from in-house engineers and additional BOMs/SBOMs from all parts/software suppliers.

b. Identify all critical components from the BOMs/SBOMs identified in 2.a.

c. Steps 2.a and 2.b would continue until the contractor/prime has obtained BOMs/SBOMs identifying every upstream input used to manufacture the critical components that make up its final product (e.g., UAS). An upstream input would be defined as a product derived from

raw materials which are commodities and do not require specialized engineering processes to manufacture or which are tamper-resistant in their final form. So, for a lithium-ion battery, the inputs of interest would include the anode, cathode, electrolyte, and all building blocks of any embedded software code.

d. The contractor/prime would then identify all critical components that could be used to maliciously interfere with the operation of the final product, its parts, or otherwise collect surveillance data as described in 1.c above.

3. CONTRACTORS DIRECT SUPPLY CHAIN AUDITS

Based on the steps listed in 2.a-d above, the contractor/prime would then be required to conduct audits of its supply chains up to its critical component/software suppliers. This is a straightforward process and requires standard audit-type checks that identify all critical component/software suppliers to ensure that they are trusted. This is accomplished through a process of:

a. inventory record checks and production schedules,

b. examinations of supplier contracts,

c. purchase order reviews,

d. sales invoice reviews, and

e. corroboration against relevant accounting legers.

With respect to the UBO of each critical component/software supplier, there are databases, such as Dun & Bradstreet, that provide ownership information. To the extent a contractor/prime is unable to find the UBO of any supplier, this gap should be reported to the U.S. Government.

PROCESS EXAMPLE: THE LITHIUM-ION BATTERY

To illustrate the simplicity of this process, we provide the example of a lithium-ion battery included in a UAS, where the lithium-ion battery is produced by a battery pack manufacturer (tier two), who sources lithium-ion cells from cell suppliers (tier three), who then source the raw material anodes, cathodes, and electrolytes from other suppliers (tier four). Because the anodes, cathodes, and electrolytes are tamper-resistant, the supply chain audit would stop after the identities of the cell manufacturers are known (i.e., tier three being the highest point in the supply chain where tampering could occur).

In this example, the UAS contractor/prime could audit its own production records as well as the production records of its lithium-ion battery pack manufacturer (or it could contract with a third-party auditor to do this). To begin, the UAS manufacturer would examine its BOMs to determine the specific type of lithium-ion batteries that it incorporated into the UASs sold to the U.S. Departments of Interior and Defense. Using the BOMs, the UAS manufacturer would then identify the unique, product-specific serial numbers associated with the batteries to identify the battery pack manufacturers. The next steps involve supply chain audits of the battery pack manufacturers. Using the same serial numbers plus relevant production/sales records, the battery pack manufacturers will be able to identify their cell providers for each battery pack produced and sold to the contractor/prime. Relevant production/sales records include those listed in 3.a-e above. Again, the lithium-ion battery supply chain trace would end at the lithium-ion cell producer because the cell producer's raw materials are tamper-resistant, meaning that the highest level in the supply chain where malicious vulnerabilities could be introduced is at the cell level. If the cell and battery pack manufacturers are non-FEOCs, then the battery supply chain check is complete and the audit is successful.

The battery's SBOM, as it is itself a nested inventory (i.e., a self-contained list of ingredients that make up software components), could itself be checked by the UAS manufacturer. Alternatively, there are firms that can review software codes to detect backdoors and potentially malicious code, and could be hired by contractor/primes to review software that is being used.

CONCLUSION: A SUCCESSFUL PILOT PROGRAM PAVES THE WAY FOR BROADER IMPLEMENTATION

The foregoing audit checks may take several weeks up to several months to complete (depending on the complexity of the supply chain). However, even for larger contractors/primes, such as aircraft manufacturers, the traces can be accomplished within a year.[9]

Again, audit results and certifications should be provided to the U.S. Government through Survey responses, and records should be kept for at least five years. Certifications should confirm the absence of any components/software provided by FEOCs. Should contractors/primes find that certain components/software were provided by FEOCs, disclosures should be provided to the U.S. Government through Survey responses, and the Government should take immediate remedial action.

This pilot project, when proven to be successful, could be extended to all U.S. government contractors/primes using the same methodology described here.

ENDNOTES

1 China Tech Threat staff drafted this paper after consulting with CTT Advisor Nazak Nikakhtar. From 2018 to 2021, Nikakhtar served as the Department of Commerce's Assistant Secretary for Industry & Analysis at the International Trade Administration (ITA). Nikakhtar also fulfilled the duties of the Under Secretary for Industry and Security at Commerce's Bureau of Industry and Security (BIS). Additionally, Nikakhtar spearheaded the United States' first-ever whole-of-government initiative to evaluate and strengthen supply chains across all strategic sectors of the economy.

2 https://www.fbi.gov/news/stories/director-wray-addresses-threats-posed-to-the-us-by-china-020122

3 https://www.youtube.com/watch?v=jk3u2sfPQAg

4 https://www.nytimes.com/2022/08/29/technology/china-semiconductors-technology.html

5 https://semiengineering.com/chip-backdoors-assessing-the-threat/

6 https://www.reuters.com/graphics/UKRAINE-CRISIS/ARMS/lgvdkoygnpo/

7 This would be much like the current self-policing prohibitions on the importation and use of items derived from forced labor or conflict minerals.

8 SBOM is "a list of all the open source and third-party components present in a codebase. An SBOM also lists the licenses that govern those components, the versions of the components used in the codebase, and their patch status, which allows security teams to quickly identify any associated security or license risks." https://www.synopsys.com/blogs/software-security/software-bill-of-materials-bom/

9 Audits may be conducted every few years depending on the nature of the contractor's/prime's operations. If, however, the contractor/prime is required by the U.S. Government to keep FEOC components/software out of its supply chains and establish a robust system to ensure ongoing compliance, then audits will not need to be conducted as frequently.

NO WEAK LINKS

A STRATEGY FOR KEEPING U.S. SUPPLY CHAINS CLEAN OF DANGEROUS CHINESE TECHNOLOGIES

IN CONSULTATION WITH NAZAK NIKAKHTAR, CHINA TECH THREAT SPECIAL ADVISOR

www.chinatechthreat.com