LIBERTY BELL PROJECT

Spies, Saboteurs, and Access to U.S. Connected Devices

Options to Address the Market Dominance of China-Made IoT Modules

by Clete Johnson
Founder, Liberty Bell Project
July 2025

Internet of Things (IoT) modules are compact hardware components embedded in most every device that can connect to wireless networks. These modules enable connectivity, and as such, they are indispensable infrastructure in our increasingly connected society. Accordingly, their security is also indispensable to the safety of almost every element of our society – from connected vehicles to energy infrastructure to medical devices to police body cameras.

China's aggressive cyber operations and the insidious risks of espionage or sabotage via IoT modules have raised alarms among U.S. policymakers, particularly about certain China-based manufacturers of these modules such as Quectel and Fibocom. The Department of Defense recently added Quectel to its "China military companies" list, indicating that Quectel can be influenced by China's defense and intelligence agencies, and the Commerce Department has undertaken two rulemaking proceedings that would address security concerns.

However, the security considerations pertaining to suppliers of IoT modules may in fact be more dire than most policymakers have considered. In fact, only three of the top 10 global manufacturers have operations that are insulated from Chinese Communist Party (CCP) influence, and one of those three, Switzerland-based u-blox, announced in January 2025 that it is exiting the IoT module market. China-based manufacturers are poised to seize near total dominance of the global market for these devices, meaning that in the near future, most every new connected device in the world could gain its connectivity through a China-made module.

This paper explores the security ramifications of this possibility. It concludes that the U.S. government should consider steps to prevent the global market for these modules from being altogether overtaken by China-based manufacturers that are the dominant suppliers of IoT modules globally and threaten to extinguish trusted competitors.

Part I provides an overview of what IoT modules are, what they do, and how sophisticated cyber-supply chain operations could affect safety and security in the physical world. Part II describes the present global market for IoT modules and provides analyses of the parallels between today's module market and the parallel global market for telecommunications infrastructure, which Huawei and ZTE have sought to dominate with support from China's government. Finally, Part III surveys the various U.S. government tools that could address this challenge, concluding with a menu of options ranging from "do nothing at all" to "fund replacements nationwide."

The Liberty Bell Project is a 501(c)(3) non-profit education and training organization whose activities and reports aim to strengthen the infrastructure of our free society; the organization does not conduct advocacy of any kind. The author has studied and worked on supply chain security for decades as a U.S. Army logistics officer, counsel to the Senate Select Committee on Intelligence, chief counsel for cybersecurity at the FCC, senior adviser to the Secretary of Commerce, and in private law practice.

LIBERTY BELL PROJECT

Part I – IoT Modules and Security Concerns in Connected Devices

A. Overview of IoT Modules and their Uses

IoT modules, which connect devices and equipment to wireless networks, are essential components for any device or equipment with wireless connectivity. IoT modules are hardware components that enable wireless communications between a wireless network and IoT devices, including smart meters, connected vehicles, connected medical devices, and equipment used in "smart" factories and other infrastructure. All these devices contain modules that are usually specially designed for particular device types. As we continue our societal march to ubiquitous connectivity, we become ever more reliant on these small pieces of hardware.

(*Module located in a connected device - photo from IoTNow*)

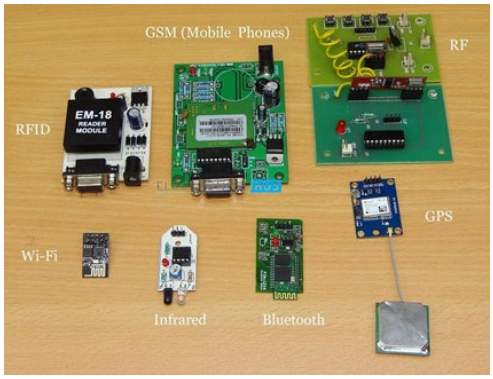
IoT modules can connect to mobile or local wireless networks. Mobile wireless networks, also known as "cellular networks," are composed of base stations such as cell towers and "small cells" that each cover a geographic area, providing mobile wireless connectivity in service areas known as "cells." Cells linked together can provide radio coverage over wide geographic areas, as cells can hand over voice and data communications to each other. Cellular networks thus enable cell phones and other transceivers to connect to wireless networks even while in motion. Cellular networks, which operate on licensed radiofrequency spectrum, are distinct from other types of local wireless networks that operate on unlicensed spectrum such as Wi-Fi, which allows devices near a wireless access point and router to access the Internet, and Bluetooth, which connects devices to other devices over very short distances. IoT modules allow devices to connect to both types of wireless networks.

IoT modules enable data transmission between devices and wireless networks by converting signals between radio waves and digital data. The modules, located on a Printed Circuit Board (PCB), are units that contain smaller components necessary for a device's wireless communications functionality, including the chipset, the radiofrequency front end, power, and memory components. One side of a module connects to an antenna, which transfers data to and from wireless networks. The other side of the module connects to the device's application processor. The application processor serves as the "brain" of the device or equipment, running the operating system, processing graphic and video data, and controlling other key functions for smart devices. (Note that depending on the module, an antenna or processor may be included within the module unit.)

For data received by the device from the wireless network, first the antenna must capture radio waves. The module then converts those analog radio waves into digital signals and translates the digital signal into information that can be understood by the application processor. For data transmitted from the device to the wireless network, the process operates in reverse; the module converts digital signals into radio waves. The antenna then transmits data through the radio waves to a base station.

In short, without a properly functioning IoT module, the device's application processor could not receive data from or transmit data to wireless networks, and the device would be useless.

Producers of IoT modules design and manufacture or source the module itself and the various components contained within the module. Due to different devices' shapes, sizes, functionality, and power needs, IoT modules are usually designed specifically for particular devices.



IoT module suppliers simplify the process of building wireless connectivity into devices and equipment. The integration of several components into a single unit, which can then be connected to other components within the device, simplifies the design process for IoT device and connected equipment manufacturers. For instance, modules need to be able to operate with all cellular networks; those that are pre-certified with cellular network operators may decrease the time and expenses of certifying the device or equipment. The largest cellular network providers in the United States have shortened certification times for devices that use pre-approved modules.

B. Cyber-Supply Chain Security Threats to IoT Modules

IoT modules are an indispensable link in connecting devices to wireless networks. All data to and from these networks must flow through and be processed by the module, which also may allow for the capability to update connected device software remotely – often without the end user's knowledge. The security of IoT modules is particularly vulnerable during the manufacturing or distribution process, as sophisticated bad actors can either manufacture modules susceptible to remote access or insert them into connected devices in the distribution process to allow for remote access by particular actors, allowing for malignant software activity. Security vulnerabilities may also arise post-sale via operations that target particular modules, including by embedding malware through firmware updates or even "human intelligence" operations as seen in spy movies – "HUMINT-enabled SIGINT" in trade parlance – in which a

trained operative conducts a highly-targeted malware placement on a single specific device or set of devices.

Modules are used by companies and people that use wireless devices – which in today's connected society means essentially every company and every person. For example, almost all vehicles manufactured today can connect to wireless networks and, of course, have modules incorporated into the vehicle. Medical equipment often uses wireless networks to allow for remote access or control of the equipment, monitor patients remotely, or transfer patient data. Connected medical devices include wearable devices, medical equipment used in hospitals such as IV pumps, and implantable devices. Additionally, the electric sector is in the process of deploying smart grid technologies, such as smart meters, to efficiently automate distribution of electricity. Likewise, gas and oil companies use IoT devices to monitor pumps and pipelines, inspect operations remotely, and analyze equipment and worker health. Sensitive public safety devices ranging from drones to police cars to body cameras depend on these modules. Wireless communications, and thus IoT modules, are a core component of thousands of types of such systems, and perhaps hundreds of millions of connected devices.

Therefore, IoT modules constitute a potential security threat vector to almost every aspect of modern life by providing an avenue for sophisticated operators to access the connected devices. This access may permit remote actors to disrupt, degrade, manipulate, or altogether disable connected devices. For instance, remote operators have disabled tractors stolen from a Ukrainian dealership using modules.

Remote actors also may access information and data from connected devices. In 2023, the UK media reported that a surreptitious Chinese module had been discovered in UK government cars, including those used by senior government minsters. The module, which was described as a "tracking device," was reportedly identified after officials had dismantled the British Government vehicles and swept them. The Cybersecurity and Infrastructure Security Agency (CISA) has identified a backdoor that enables "patient data spillage" in a healthcare patient monitor made in China.

Even without remote access to the module, though, suppliers of IoT modules can arrange for access to data collected downstream by IoT devices and process that data for other uses. The Australian Strategic Policy Institute explains how Chinese entities use commercial partnerships to collect data for China-based technology companies.

Remote access to or disruption of modules in connected devices and equipment could significantly impair the safety and security of Americans and the United States as a whole. Access to or disruption of connected devices and equipment could result in loss of life, damage the U.S. economy, or the exfiltration of sensitive and confidential information about individuals, critical infrastructure, or government, military, and law enforcement operations.

Despite these risks and the importance of wireless connectivity to the U.S. economy, we rely largely on IoT module manufacturers based in China, a designated "foreign adversary" of the United States. The Department of Commerce's Bureau of Industry and Security (BIS) already has identified the threats that arise from China's role in the supply chain for connected vehicles –

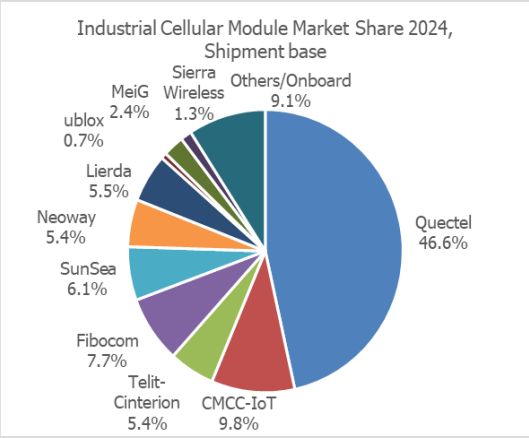
that is, almost all vehicles manufactured today. As discussed further below, China's role in supply chains for wireless devices presents significant risks and challenges for the United States.

Sophisticated adversary intelligence services – China's, Russia's, Iran's, North Korea's – and many of their criminal proxies possess the capability of conducting cyber-supply chain espionage or sabotage operations, through remote access, firmware updates, or targeted HUMINT-enabled SIGINT. To be clear, the answer to the question of whether these intelligence services and criminal proxies – particularly China's – would leverage such capabilities is simply: Of course they would. To put it bluntly, they have done so already, and they will continue to do so. In assessing threats, security personnel look to both intent and capability. Adversary intelligence services like China's possess both; the threat is clear and present.

This is not a scenario in which a skeptic might reasonably ask, "But is there actually a 'smoking gun' that shows that China has taken such actions?" China's cyber operations, particularly against the United States, are the most voracious and aggressive such operations in the world. As we will discuss further below, the extraordinary reach of China's IoT module manufacturers into the global connected devices market provides China's intelligence services innumerable opportunities to access those devices through either cyber or human operations or both.

Part II – The Possible Chinese Takeover of the Global Market for IoT Modules

A. Overview of the Global IoT Module Market and China-Based Manufacturers



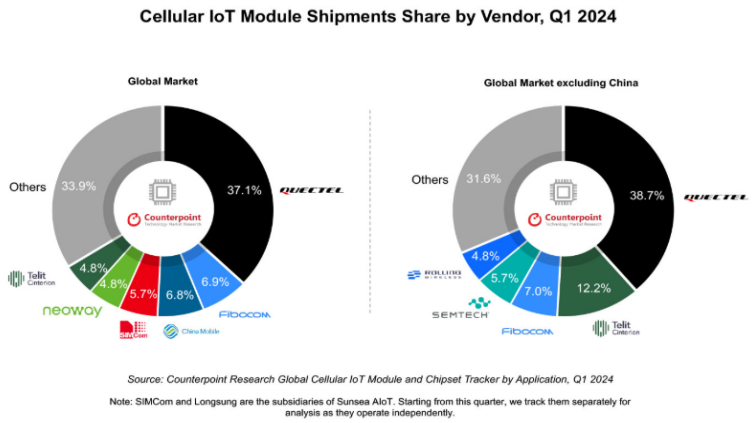
https://iotbusinessnews.com/2025/02/19/02010-2024-cellular-iot-module-market-update/

As smart devices become more ubiquitous in our daily lives, so too will IoT modules. For that reason, it is important to understand the supply chain for these digital components. As demand inevitably rises, more companies will be looking to IoT module suppliers to fulfill their production needs. As we demonstrate below, China-based manufacturers are the dominant suppliers of IoT modules globally and threaten to overtake the entire global market and extinguish trusted competitors.

While publicly available sources differ on the exact market breakdown, they agree on one key point: Quectel leads the market by wide margins. According to GlobeNewswire, the top five IoT module vendors in 2024 were: Quectel (China), Fibocom (China), Telit Cinterion (U.S.), Semtech (Canada), and u-blox (Switzerland). Together, these five companies account for 72% of the global market share in terms of revenue. According to another source, however, Quectel, Fibocom and China Mobile are the leading module manufacturers, collectively holding a 50% global market share in Q1 2024; all three of these companies are based in China. For markets *excluding China*, Telit Cinterion, a U.S. based company, holds the number two spot behind Quectel with 12% market share. Below, we provide additional information on the market share of some of the biggest players in the space:

- *Quectel (China).* Quectel is the global revenue leader by far. According to IOT Analytics, it has a 31% market share, and continues to grow, with 19% year over year growth based on revenue as of Q1 2024. Other sources indicate that it has as much as 46% of the market.
- *Fibocom (China).* Fibocom holds about a 10% market share and reported a 10% increase in revenue in Q1 2024 year over year.
- *Telit Cinterion (U.S.).* Telit Cinterion holds a 7% market share and reported a 23% year over year decline in revenue as of Q1 2024. For markets excluding China, Telit Cinterion has about 12% market share.
- *Sierra Wireless/SEMTECH (Canada/U.S.).* Semtech has a 3% market share and reported a 39% year over year decline in IoT module revenue 2023-2024. [Techno Systems Research, 2024-2025 Cellular Broadband Device & Module Market Data, rev 1.3.]
- *U-blox (Switzerland).* In January 2025, u-blox announced its strategic decision to phase out its IoT module business, and will therefore be exiting the market soon. In March, it announced plans to divest the module business to Trasna, which is headquartered in Ireland, with innovation hubs in France, Dubai, India, and Tunisia.

While Chinese sources of IoT modules are gaining, non-Chinese sources are declining if not departing the market altogether. Regardless of whether these two trends are related, it is clear that the two groups are headed in opposite directions, with Chinese companies ascendant.



https://www.counterpointresearch.com/insights/global-cellular-iot-module-market-q1-2024/

Other Players. There are a number of other smaller players in the IoT module market, including several other China-based companies such as China Mobile, SunSea, Neoway, MeiG, Lierda, and Rolling Wireless. Mo-Magic, an India-based company, and Sirin Software, a Ukrainian company, are also participants in the market.

If China-based companies continue to increase global market share and to dominate the supply chain, the U.S. may become dependent upon China for IoT modules precisely at a time when we are growing more reliant on smart devices and embedding such technologies into virtually every aspect of our day-to-day lives. As discussed below, the ascendence of China-manufactured modules is a result of a strategic CCP plan to promote Chinese companies as global market leaders in this field.

B. Analysis of Similarities Between Quectel and Huawei in Market Approach

China wishes to dominate the IoT module market for strategic reasons. The CCP views communications equipment and data as strategic assets, and China's domination of the global

IoT module market would provide a firm grip on networks, devices, and the data that they produce. In 2009, the Chinese government decided to allocate significant financial resources to the development of the IoT sector. In 2012, the Ministry of Industry and Information Technology stated that IoT was "strategic high ground" and defined priorities that have guided its development in China, including concentration of research and development efforts. In the 13th Five Year Plan (for years 2016-20), China articulated goals around developing and promoting IoT infrastructure and applications, encouraging breakthroughs in chips and key components of cybersecurity, and strategic initiatives for data collection and use.

This type of strategic planning in the technology sector is not new to China, whose technology strategy benefits from China's scale, centralization, and industrial capacity. In fact, it ran a similar playbook to enable the rise of Huawei, China's "national champion" telecommunications behemoth. The Chinese government implemented subsidies and other strategic support, which played a part in Huawei's rise as a leader in the 5G space. For example, in 2020, China announced investments of $1.4 trillion over six years to boost Chinese technology companies like Huawei in their pursuit to lay 5G wireless networks and install surveillance technologies globally. State-owned Chinese banks provided large amounts of capital to Huawei, which in turn empowered the company to offer lower prices than its competitors to rise as the market leader.

The purpose of this strategic support for Huawei was partially commercial; of course, China's government wants China-based companies to prosper worldwide. But beyond that, China seeks to leverage the surveillance and security benefits from having its leading telecom equipment company build communications infrastructure throughout the world. While Huawei is nominally a private company, China's national security laws require all organizations and individuals to accede to requests from security authorities. This reporting requirement – indeed, subservience to the CCP – is fundamentally different from the relationship between companies organized under the laws of the United States and its market democratic allies. To put it simply, this law and the authoritarian CCP governance culture that undergirds it provide China's intelligence services potential access to – and even control over – any Huawei-built network in the world.

Most cyber intelligence operations require a sophisticated plan to "break into" a network or to activate a so-called "back door," but for China's intelligence services, a Huawei network allows government officials to gain access simply by requirement. They need not break in or create a back door; they need only ask for the keys to the front door. In contrast, in the United States and other free societies, government entities generally undergo rigorous vetting by an independent judiciary to obtain a warrant to intercept private communications.

Similarly, China now aims to establish a monopoly on IoT modules which are vital components of the modern economy. China plans to achieve this monopoly through China-based companies such as Quectel and Fibocom. Through the tried-and-true strategy of combining government subsidies, access to cheap and vast amounts of capital, and ongoing state support both in China and worldwide, China is pursuing a goal of driving other nations' suppliers out of business.

This government strategy has already been extraordinarily successful. According to research firm IoT Analytics, neither Quectel nor Fibocom had any presence at all outside China in 2016, but by 2022, they had ascended to the top two positions in global market share outside China,

placing Quectel on top with 29 percent and Fibocom second with 13 percent. These companies hold similar positions today. According to Counterpoint Technology Market Research, Quectel is the leading supplier in every major market region in the world, ranging from 22 percent of the market in North America to 61 percent of the market in the Middle East and Africa.

With u-blox's decision to exit the market, it seems that China is on its way to meeting its goals to dominate the global market for IoT modules. Dependency on China-based companies like Quectel, Fibocom, Sunsea, Neoway, and MeiG for IoT modules provides an avenue for potential adversary intelligence access to – and espionage and sabotage of – every device that includes their modules. Accordingly, as discussed below, the U.S. Government has declared through various actions in multiple agencies that this constitutes a grave threat to U.S. security.

Part III - U.S. Government Tools and Possible Policy Actions

In August 2023, Representatives Mike Gallagher (R-WI) and Raja Krishnamoorthi (D-IL) of the House Select Committee on the Chinese Communist Party wrote a letter to then-Chairwoman of the Federal Communications Commission (FCC) Jessica Rosenworcel requesting information about the threat of Chinese IoT modules. They explained that insecure modules:

> "have the capacity both to brick the device and to access the data flowing from the device to the web server that runs each device. As a result, if the CCP can control the module, it may be able to effectively exfiltrate data or shut down the IoT device. This raises particularly grave concerns in the context of critical infrastructure and any type of sensitive data."

Specifically, they raised concerns about Quectel and Fibocom. Then-Chairwoman Rosenworcel responded with a letter outlining the FCC's actions in support of this goal. Rosenworcel explained that the FCC does not have the unilateral authority to add entities to the Covered List, but must instead refer the matter to executive branch security agencies, which are presently examining these concerns from multiple angles.

A. Pertinent U.S. Government Activities, Policies, and Laws

The U.S. Government has developed a range of tools to address threats posed by untrusted information and communications technology (ICT) suppliers; these policy tools may be applied to IoT modules. Many of these tools take the form of designations or lists of individual entities or equipment and services found to pose an unacceptable threat – such as the Department of Homeland Security's (DHS) Binding Operational Directives, the FCC Covered List, the Department of Defense's (DOD) "Chinese Military Companies List," and the Department of Commerce Entity List – but the government has also begun to develop class-based prohibitions under the new BIS Information and Communications Technology and Services (ICTS) transaction review process. While the DHS and DOD lists focus on prohibitions in federal procurement, the BIS Entity List, the FCC Covered List, and BIS ICTS transaction reviews apply to the broader commercial market.

We provide an overview of each of these mechanisms below.

Department of Commerce BIS Entity List. The Export Administration Regulations (EAR) contain a list of names of certain foreign persons – including businesses, research institutions, government and private organizations, individuals, and other types of legal persons – that are

subject to specific license requirements for the export, reexport and/or transfer (in-country) of specified items so that U.S. technology that could be used for nefarious purposes does not fall into the hands of bad actors. These persons comprise the Entity List, which is found in Supplement No. 4 to Part 744 of the EAR, and they are subject to licensing requirements and policies supplemental to those found elsewhere in the EAR.

FCC Covered List. The FCC Covered List currently identifies equipment and services from ten Chinese entities and one Russian entity, as well as their subsidiaries and affiliates. The FCC prohibits the use of Universal Service Fund resources and other FCC subsidies for equipment and services on the Covered List, and the agency is administering a reimbursement program to compensate small carriers for the cost of removing, replacing, and disposing of such equipment. The FCC also prohibits authorization of equipment that has been identified on the Covered List, effectively banning such products from the U.S. market because authorization is necessary to market or operate RF equipment in the United States.

Kaspersky ICTS Final Determination. On September 13, 2017, DHS issued a Binding Operational Directive directing the removal of Kaspersky-branded products from federal networks and prohibiting federal departments and agencies from purchasing those products going forward. On June 20, 2024, BIS announced its first-ever Final Determination, under the authority of E.O. 13873, prohibiting Kaspersky products from being provided in the United States and to U.S. persons. In making the Final Determination, BIS determined that Kaspersky poses an undue or unacceptable risk to national security because Kaspersky:

1. Is subject to the jurisdiction of the Russian government and must comply with its requests for information;
2. Has access to sensitive U.S. customer information through administrative privileges to U.S. systems;
3. Has the ability to use its products to install malicious software on U.S. customers' computers or selectively deny updates, leaving U.S. persons and critical infrastructure vulnerable; and
4. Cybersecurity software is integrated into third-party products and could be unwittingly introduced into devices or networks containing highly sensitive U.S. persons data.

Following the Final Determination, the FCC also added Kaspersky to the Covered List. We note that the security concerns related to Kaspersky software also apply to security concerns related to IoT modules made by China-based hardware manufacturers.

Connected Vehicles. On January 16, 2025, BIS published its first class-based transaction ban with the Connected Vehicle Supply Chain Final Rule, prohibiting transactions involving vehicle connectivity system (VCS) hardware and covered software designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of China or Russia. This rule also requires VCS hardware importers and connected vehicle manufacturers to submit to BIS Declarations of Conformity, provides a mechanism for BIS to issue general and specific authorizations, and establishes advisory opinion and appeal processes. The Final Rule went into effect on March 17, 2025, but may be refined before its full implementation in vehicle model years 2027 and 2030. Indeed, BIS has already released two

general authorizations (for limited use cases and temporary importation). In the meantime, the FCC has sought input on whether and how to add these products to the Covered List.

Connected UAS. In December 2024, BIS published its final rule (effective February 4, 2025) that finalizes the practices guiding review of ICTS transactions. The final rule clarifies the federal interagency process for initial and final determinations, for example, explaining that the Secretary of Commerce is the final arbiter of decisions under the rules and that interagency consensus is not required. On January 3, 2025, BIS released an Advance Notice of Proposed Rulemaking (ANPRM), seeking comment on issues related to transactions involving foreign adversary ICTS integral to unmanned aircraft systems ("UAS"). The ANPRM sought comment on: (i) the definition of UAS and other terms; (ii) risks associated with UAS; (iii) threats posed by foreign adversaries; (iv) UAS vulnerabilities that foreign adversaries could exploit; (v) processes and mechanisms BIS could implement to authorize otherwise prohibited transactions; and (vi) the economic impact of UAS and UAS supply chain abuse by foreign adversaries. Based on stakeholder feedback and their internal review, BIS may proposal another set of class-based transaction restrictions.

The 1260H Chinese Military Companies List and Secondary Procurement Ban. Section 1206H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (FY2021 NDAA) requires the Secretary of Defense to identify each entity, operating directly or indirectly in the U.S., that is a Chinese military company. The term "Chinese military company" means an entity that is directly or indirectly owned, controlled, or beneficially owned by, or acting on behalf of, the People's Liberation Army or any other organization subordinate to the Central Military Commission of the CCP; or identified as a military-civil fusion contributor to the Chinese defense industrial base. On January 7, 2025, DOD released a notice of its annual designation of "Chinese military companies." Notable listed companies for the communications sector include Quectel. DOD may not enter into procurement contracts with identified Chinese military companies, effective June 30, 2026 for direct procurement of goods or services from a listed entity, and effective June 30, 2027 for secondary procurement (i.e., procurement of goods or services from a non-listed entity "that include goods or services produced or developed by" a listed entity).

* * * * *

Collectively, these authorities provide a mechanism for excluding or placing conditions on transactions and uses involving untrusted ICTS suppliers. Notably, the ICTS transaction review authorities also allow for the Commerce Department to require mitigations for threats posed by specific suppliers, although it has not done so to date. Other recent developments, for example in Team Telecom reviews and under the Department of Justice's new Sensitive Data Rules, provide security mitigations for certain kinds of restricted transactions. Below we consider how these tools may be brought to bear via a range of policy options to address untrusted suppliers of IoT modules.

B. Menu of Policy Options to Address or Mitigate National Security Risks

The U.S. government could consider undertaking the following steps to address the threat of China-based IoT module manufacturers. We provide this list in ascending order of aggressiveness, ranging from "do nothing at all" to fully prohibit and fund replacement of

untrusted modules. Many of these options are not practically feasible or otherwise not advisable, but for reference purposes we provide the full menu of options to show the ascending order of potential steps the U.S. government might take.

Option #1: Do nothing.

Taking no further action beyond the present listing of Quectel on the 1260H DOD list and simply waiting for the secondary DOD procurement prohibition to take effect in June 2027 is, of course, the most passive and least disruptive option. With u-blox having announced its departure from the market in January, it is not clear that the remaining trusted suppliers in the market today will still be viable in 2027.

Option #2: Manufacture China-based designs in the United States.

The next most passive option is to manufacture China-designed modules in the United States. In essence, this would be a white-labeling pass-through exercise, allowing untrusted Chinese modules to be made in the United States. While this approach could complicate some human operations that China's intelligence services might seek to conduct, it would not provide much additional security to the modules produced; in fact, it would likely provide a false sense of security, or worse, a U.S. disguise for China's intelligence operations. China's human and technical intelligence operations are extremely sophisticated; unless the U.S. personnel, facilities, equipment, and networks in question were sealed off from all virtual or personal contact with the China-based company that designed the modules, we are not aware of counter-intelligence methods that could protect against such a white-labeling approach to Chinese modules.

Option #3: Public funding for new trusted manufacturing.

Expanding subsidies for trusted manufacturing in the United States or allied countries, similar to the approach in the CHIPS Act, could provide incentives for trusted alternatives to China-made modules. This would require a large new legislative effort. In the current political and budget environment, it is not clear whether there is a path for such an initiative.

Option #4: Targeted prohibitions or restrictions.

Either through ICTS transaction review action or through the FCC Covered List (or both), the U.S. government could prohibit or otherwise restrict China-made modules in certain market sectors or for certain uses, either by named company or as a class of China-made modules. This approach would reflect the path that BIS has taken to date with connected vehicles and UAS.

Option #5: Broad prospective prohibitions, with a transition/attrition period.

Either through ICTS transaction review action or through the FCC Covered List (or both), the Government could prohibit *all* such modules in the future, again either by named prohibited companies or as a class of prohibited China-made modules. This would be similar to how the FCC Covered List has operated, rendering listed companies ineligible for FCC equipment authorization. Such action does not formally prohibit continued use of *previously authorized* modules, but it would complicate their continued use in many cases.

Option #6: Retroactive ban from the U.S. market and funded "rip and replace."

Either through ICTS transaction review action or through the FCC Covered List (or both), the government could prohibit all such modules and require that existing modules be removed from and replaced for devices in the United States. This would be similar to the "rip and replace" program, in which Congress required – and provided reimbursement for – replacement of all Huawei and ZTE communications equipment in communications networks in the United States. Beyond the budget considerations of replacing modules in U.S. devices – or in most cases, replacing the entire device in which the module is embedded – it is difficult to imagine the practical completion of such an effort with tens of millions of devices.

Conclusion

Security for our modern connected society requires security of IoT modules. Given China's aggressive cyber posture and its intelligence agencies' sophisticated capabilities to reach U.S. infrastructure through cyber-supply chain operations, U.S. policymakers have sounded the alarm about China's IoT module manufacturers. This paper has explained why these concerns are well-founded, and how the security situation could worsen. It recommends that the United States consider steps to prevent the global market for modules from being completely overtaken by China's "national champions." Ultimately, the U.S. government must bring the full breadth of its intelligence and security assessments to bear in considering how best to address this complex threat most effectively, and we recommend that it do so via an open and transparent process with trusted stakeholders and in coordination with like-minded partners and allies.