DECEMBER 2022

Improved Export Controls Enforcement Technology Needed for U.S. National Security

By Gregory C. Allen, Emily Benson, and William Alan Reinsch

Executive Summary

As technology has become increasingly central to strategic competition with Russia and China, export controls have moved to the forefront of U.S. foreign policy on technology issues. Most notably, restricting Russia's access to advanced technology through export controls is a key part of the U.S. response to Russia's invasion of Ukraine, as U.S. government officials have repeatedly stated.

Unfortunately, nearly all the debate is focused on whether and when to apply export controls, not how to ensure that export controls are effectively administered and enforced once applied.

The Bureau of Industry and Security (BIS) at the Department of Commerce oversees most export controls. Unfortunately, BIS is increasingly challenged by worldwide smuggling and export control evasion networks, especially those that are supported by Russia and China. Investigators have examined the wreckage of downed Russian weapons systems in Ukraine and found that they contain U.S. and allied components, including electronics that were manufactured years after the implementation of the 2014 Russia export controls.

Given the dramatically expanded anti-Russia export controls of 2022, Russia is certain to devote significantly more resources to evading these controls to keep its war machine and economy functioning. As Russia pursues increasingly aggressive and better-resourced means of obtaining critical technology, BIS must use every tool available to increase capacity and productivity for effective enforcement. Ongoing efforts to starve Russian military forces of advanced technology underscore the urgency behind reevaluating the current export enforcement regime and fortifying its capabilities for a new and more complex geostrategic environment.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

In October 2022, the Biden administration further expanded the scope of U.S. export controls when it released two new rules aimed at severely restricting Chinese artificial intelligence (AI) and semiconductor capabilities. A recent CSIS report, *Choking Off China's Access to the Future of AI*, assesses these controls in detail. What is novel about these controls is that they represent a sea change in the U.S. approach to China, particularly since the controls are both geographic in nature and unilateral. The administration has also indicated recently that it is shifting from a policy focused on delaying adversaries' technological advancements to one of directly degrading them. Though less severe than those imposed on Russia, these new export controls are intended to prevent China from achieving key strategic priorities. Both Russia and China are doubtless devoting massively increased resources to evading the new export controls.

At a time when the need for robust U.S. export controls is more strategically critical than at any time since the end of the Cold War, BIS's enabling technology is in a dreadful state. The cause is simple: decades of underinvestment. Current and former BIS staff state that the major government databases that they use to monitor trade flows and identify suspicious activity can perform only a fraction of the needed functionality and crash routinely. Instead of knowledge graph databases and machine learning—capabilities that have revolutionized both the private sector and other federal agencies with similar missions—BIS analysts perform their work primarily using Google searches and Microsoft Excel.

Modern, data-driven digital technologies utilizing AI and machine learning can and should play an integral role in enhancing BIS export control enforcement capabilities. Relatively modest investments could lead to 5 to 10 times greater analyst productivity. Despite the increasingly pressing need to invest in these new enforcement capabilities, the budget of BIS has not increased commensurate with the increased number of export-controlled items, the evolving threat landscape, and the growing pressure from an increasingly sophisticated evasion regime.

The current international momentum behind U.S.-led export controls presents a unique opportunity both to help solve a pressing problem—responding to Russia's invasion of Ukraine—and to advance the adoption of digital technology by U.S. government agencies for mission impact. A changed geopolitical landscape demands reinvigorated U.S. government export controls capacity, and this cannot be done without additional resources. CSIS analysis of relevant comparable data-driven digital technology modernization efforts by other U.S. government agencies with similar mission requirements suggests that this could be accomplished with an additional appropriation for technology modernization at BIS of roughly $25 million annually for five years. This funding would allow BIS to better ingest, connect, and analyze hundreds of billions of records from both government and open-source data. By applying modern data science and machine learning techniques, BIS could increase productivity across all its processes: for example, automatically detecting that a purported Eastern European "tractor manufacturer" has the same phone number as a supplier of engines to the Russian military. This figure accounts for opportunities at BIS to improve collaboration with other U.S. government agencies and the need to prevent unnecessary duplication of effort.

However, a more productive enforcement analysis community will identify more entities as likely shell companies engaging in illicit transactions. This will in turn increase the need for enforcement agents to conduct site inspections or criminal investigations of these identified entities. Despite the severe current technological limitations on the efficacy of the analytic community, its work is already identifying enough candidate entities for inspection to more than fully consume the capacity of the current staff. Therefore, in addition to the $25 million annual increase for five years to support new technology and staff for BIS analytical capabilities, BIS will also require an additional $18.4 million and 48 positions annually for the Export Enforcement organization as well as another $1.2 million for additional classified facility space for

these individuals to support the classified aspects of their work. Thus, the total size of the recommended additional BIS budget appropriation is $44.6 million annually.

In terms of return on investment, this increase in BIS's budget by $44.6 million annually is likely to be one of the best opportunities available anywhere in U.S. national security. The U.S. government is currently spending tens of billions to assist Ukraine in destroying the weapons of Russia's military, which too often are powered by U.S. technology. Providing a few tens of millions of dollars annually to BIS to modernize the technology that enables export controls enforcement would go a long way toward ensuring that far fewer Russian and Chinese weapons using U.S. technology are built in the future.

Report

As technology has become increasingly central to strategic competition with Russia and China, export controls have moved to the forefront of U.S. national security.

After the end of the Cold War, export controls became a somewhat niche topic within U.S. national security policy, focused principally on regulating sales of military items and restricting the spread of weapons of mass destruction. Controls on dual-use technologies, those that can be used for both military and commercial purposes, sought to balance the national security benefit of restricting sales with the parallel goal of enabling high-technology companies to maintain revenue streams from exports that supported their development of next-generation technologies.

However, this changed with the run-up to Russia's unlawful invasion of Ukraine in February 2022. Speaking on behalf of the Biden administration on February 23, Deputy Treasury Secretary Wally Adeyemo **said**:

> The key thing that [Russian] President Putin needs to consider is whether he wants to ensure that Russia's economy is able to grow, that he has the resources he needs to be able to project power in the future. If he chooses to invade, what we're telling him very directly, is that we're going to cut that off.
>
> We're going to cut him off from Western technology that's critical to advancing his military, cut him off from Western financial resources that will be critical for feeding his economy and also to enriching himself.

As Adeyemo's statement indicates, the United States views technology export controls not only as a defensive measure to limit the spread of weapons but as a powerful tool of national security—capable of deterring or punishing actions contrary to U.S. and allied interests. When the United States and its allies did successfully agree on a multilateral regime of export controls against Russia, export controls moved back to the forefront of U.S. national security policy.

In September 2023, National Security Advisor Jake Sullivan **said** that the Russian export controls "demonstrated that technology export controls can be more than just a preventative tool. If implemented in a way that is robust, durable, and comprehensive, they can be a new strategic asset in the U.S. and allied toolkit to impose costs on adversaries, and even over time degrade their battlefield capabilities."

More recently, on October 7, the Biden administration enacted a major set of export controls that restricted the sale of AI and semiconductor technology to China. The new export controls dramatically reduce China's prospects for becoming a superpower in AI technology and likewise reduce China's prospects for being self-sufficient in semiconductor technology.

When targeted correctly and enforced effectively, export controls are a powerful tool of foreign policy, as seen in the 2018 restrictions on semiconductor sales to ZTE and Huawei.

Export controls are critical to competing in this new era. Though the Biden administration's threats of export controls and sanctions did not successfully deter Russia's 2022 invasion, there is ample recent evidence of their power. In 2018, Huawei and ZTE were China's first- and second-largest telecommunications equipment companies, respectively. However, the United States imposed export controls on ZTE in 2018 and Huawei in 2020. In ZTE's case, the export controls were a penalty for violating the terms of an earlier settlement. In a matter of months, the ZTE order, which, along with other restrictions, prevented the company from buying U.S.-designed semiconductors, rapidly transformed ZTE's financial situation from significant profitability and rapid growth to imminent bankruptcy. Huawei, for its part, lost access to U.S. semiconductor design software. As a result, Huawei's smartphone chip design subsidiary, HiSilicon, was forced to halt most operations, and Huawei is no longer one of the five largest global smartphone manufacturers.

The Huawei and ZTE export controls were a potent reminder to the U.S. foreign policy community of the power of export controls. U.S. technology export controls were able to do significant damage to the financial prospects of leading Chinese technology giants. The United States did this entirely with non-violent means and at a limited cost to the U.S. economy.

However, major weaknesses in U.S. export control enforcement capacity are evident, as demonstrated by Russia's success in evading controls for weapons used in Ukraine.

There is a risk of drawing too much optimism from examples such as Huawei and ZTE. The concentrated nature of the advanced semiconductor manufacturing sector made these controls easier to enforce than many others. Additionally, export controls are, in some ways, like a sawblade that can become duller and less effective with repeated use. It remains critical that export controls are not only applied strategically and judiciously but that sufficient resources are also devoted to re-sharpening the blade.

As every street corner narcotics dealer knows, there is a major difference between a business transaction being illegal and it being impossible. The U.S. export licensing and administration process determines whether or not an international sale by a U.S. entity is permissible, but the efficacy of enforcement of the controls determines whether or not such sales will succeed when they are attempted and whether the terms of the license are honored subsequent to export. There are a variety of tactics that illicit actors can use to gain access to U.S. technology in defiance of export controls, ranging from outright theft and smuggling to the use of shell companies that hide the identity of an unlawful end user behind a front company falsely purporting to be purchasing the item legally. Former Department of Commerce and U.S. intelligence community officials interviewed for this project said that it can sometimes take the Russian and Chinese military mere days to successfully set up a shell company for purchasing U.S. technology, while the current process for uncovering a shell company's illegal activity may take years, if it is uncovered at all.

Russia's invasion of Ukraine has offered new opportunities to assess the technologies being used in Russian military systems and therefore the efficacy of prior export controls. Research by Conflict Armament Research (CAR), a UK-based investigative organization that analyzes supply chains from the weapons recovered from conflict zones, has worked with the Security Service of Ukraine to analyze Russian weapons used in that conflict. CAR's investigation found that the "Russian military industry had been able to obtain key components for UAVs—such as GPS modules, electronic parts, cameras, and engines—from Asia, Europe, the Middle East, and the United States, both before and after the start of the conflict in Ukraine in 2014."

This is important because the United States significantly expanded export controls on sales to Russia of many dual-use technologies following Russia's initial invasion of Eastern Ukraine in 2014 and military support to separatists, particularly the Western microelectronics that Russia is heavily dependent on for its advanced weapons systems. Damien Spleeters, one of the authors of the CAR study, said in an interview that markings on some of the Western-produced electronics indicated that they were manufactured years after 2014. "It's significant for me because it shows that even after Russia took Crimea and the first package of sanctions were taken against them, they still managed to acquire critical technology, critical components for important pieces of equipment that they are now using against Ukraine," he said.

Other organizations examining Russian weapons from Ukraine have produced more evidence of the same conclusion. A report by the Royal United Services Institute for Defense and Security Studies (RUSI) found that:

> RUSI discovered at least 450 different kinds of unique foreign-made components across these 27 systems. . . . Of these, at least 80 different kinds of components were subject to export controls by the US, indicating that Russia's military–industrial complex has, in recent decades, been able to successfully evade US export controls.
>
> . . .
>
> Western-designed components found in a Kalibr cruise missile, for example, appear to date to 2018 and 2019—four years after a wide range of sanctions and export controls targeted Russian military end users following the Kremlin's invasion of Ukraine.

RUSI also found evidence of Russians having scratched out identification markings on the components, indicating deliberate efforts to make it more difficult for investigators to determine how export controls are being successfully evaded.

To be clear, the findings by both CAR and RUSI suggest that the majority of U.S. microelectronics being used by the Russian military were likely acquired prior to the expansion of export controls in 2014, when doing so would have been much easier, though still disallowed in cases where the end user was known to be a military entity. However, their findings demonstrate that Russia has successfully continued acquiring such technology even after export controls were expanded in 2014.

Following Russia's enlarged invasion of Ukraine in early 2022, the United States and its allies enacted a far stricter regime of export controls and sanctions against Russia that will, in many ways, be far more difficult to evade. Despite this, the Russian defense sector continues to express optimism about its ability to evade export controls. For example, the president of Kalashnikov, a major Russian weapons manufacturer, recently said, "[There are] no problems getting [chips], because the component base cannot be 100% closed off to Russia. It is impossible to isolate Russia from the entire global electronic component base. It's a fantasy to think otherwise."[1]

Similarly, recent U.S. government export control policy changes have included acknowledgments that prior efforts against China's military often have been ineffective.

On October 7, 2022, the Department of Commerce announced major changes to export control policies toward China for the procurement of advanced AI and semiconductor technology used in both commercial and military AI systems. This policy document included important acknowledgments that previous export control approaches—based on restricting the sale of dual-use technologies to military end users or for military

1. Translation by Samuel Bendett, a native Russian speaker and an analyst of Russian military technology, available at https://twitter.com/SamBendett/status/1557350269146521601?s=20&t=LYSB23e_WNaNdj87GRC1QQ.

end uses—had diminished in effectiveness over the past decade. Specifically, the new policy stated that controls prior to October 7 "generally only apply when the 'U.S. person' has knowledge that their activities are contributing to prohibited end uses or end users. China's military-civil fusion effort makes it more difficult to tell which items are made for restricted end uses, thereby diminishing the effect of these existing controls."

The difficulty of enforcing these controls effectively is also evident from examinations of Chinese military equipment procurement efforts. Researchers at the Center for Security and Emerging Technology (CSET) analyzed 24 public procurement contracts awarded by the Chinese military and state-owned defense companies for AI-related military systems. CSET found that nearly all the identifiable chips in military procurement records were designed by U.S. companies and successfully purchased in defiance of U.S. restrictions. In other words, in each of these cases, the Chinese military was openly advertising its intention to circumvent U.S. export controls and evidently was able to successfully do so, most likely by hiding the purchases for military end users behind Chinese academic or commercial shell organizations.

While the CSET study was focused on the recent procurement of AI chips, the U.S. government has been expressing concern for years that China is too often succeeding in evading export controls on a much broader range of technologies. BIS has some flexibility to change its approach to regulation in order to make enforcement easier and more effective, as it did with the October 7 regulatory changes, but only Congress can appropriate additional resources for export license application review and export control enforcement.

Given the dramatic recent expansion of U.S. and allied export controls against Russia and China, these countries are certain to be massively increasing efforts to evade such controls.

Two of the largest expansions of U.S. and allied export controls in decades occurred in 2022: those targeting Russia in response to its invasion of Ukraine and those targeting China in response to its AI military modernization efforts and military-civil fusion policy.

If successfully enforced, these export controls would be devastating to both countries. Russia needs Western technology in order to continue manufacturing weapons to wage its war in Ukraine and also to prevent an economic disaster. While the new recent export controls against China are not an existential threat to the regime or even a major effort at decoupling China from the U.S. economy, they are a direct attempt to stop the Chinese government from achieving two of its top priorities: AI excellence and self-reliance in semiconductors. AI was the top technology priority listed in the Chinese government's five-year economic plan for 2021 to 2026, and achieving self-reliance in semiconductors has been a major feature of Xi Jinping's speeches since he became general secretary of the Chinese Communist Party in 2012.

From the perspective of China and Russia, U.S. export controls are inflicting tens of billions of dollars of economic pain, an even greater amount of lost future economic growth potential, and threatening critical strategic objectives. All of these losses represent the opportunity for a huge return on investment for Chinese and Russian organizations that successfully evade these export controls. While there is no realistic way to reliably measure how much Russia and China are increasing their investment in export control evasion activity, there is every reason to suspect that both countries are massively increasing such investments. Russia, in particular, has passed laws that are explicitly intended to assist its companies with violating foreign trade restrictions. For example, in March 2022, Russia passed laws that make it legal to import most export-controlled goods without the trademark owner's consent and to violate many foreign intellectual property rights.

Therefore, it is premature for the United States to suggest that its recent export controls on Russia will achieve its intended objectives without additional resources for enforcement.

To date, U.S. government officials have expressed significant optimism that export controls are achieving their intended objectives of cutting Russia off from Western technology that is needed for economic growth and military power. In a June 2022 interview, Secretary of Commerce Gina Raimondo stated that the controls were causing a chip shortage that was "crippling" the Russian military: "U.S. exports to Russia in the categories where we have export controls, including semiconductors, are down by over 90 percent since Feb. 24. . . . So that is crippling."

Raimondo's statement is consistent with published government trade data, though the picture is slightly better for Russia once data from countries other than the United States are included. Bruegel, a European economic think tank, analyzed data on exports to Russia from 34 countries and found that Russian imports of computers, telecommunications equipment, and microelectronics declined by 75 percent between December 2021 and April 2022 before increasing slightly in June. That said, official figures do not always tell the whole story, as they rarely include illicit transactions.

Even some of the legal data that is available gives cause for concern, suggesting that Russia is diverting its trade through other third-party countries that continue to do business with both Russia and the West. This includes falsely labeling shipments as non-controlled goods and buying finished goods that contain controlled microelectronics and stripping those goods for parts. For export control enforcement organizations, such activities are difficult to track at the required speed and scale.

There is no doubt that U.S. and allied export controls have made life harder for Russian weapons manufacturers, but it is premature to say that they are "crippling" the Russian war machine. Over time, whatever effect the controls are having is as likely to weaken as it is to strengthen. Enforcement has been difficult and will only become more complicated over time as Russian and third-state evasion tactics become increasingly advanced. As one interviewee for this project said, "As you get better at picking the low-hanging fruit, your adversary has an incentive to get more sophisticated. [Russian networks] have the benefit of the Soviet Union experience with a long history of export control evasion."

The October 7, 2022, package of export controls against China is too new for comparable data to be available at the time of this writing, but the same caution applies: published government data does not necessarily tell the whole story, which must focus on both licit and illicit transactions.

For BIS, the scale and complexity of U.S. export control requirements have increased massively over the past three years due to new legislative and executive requirements.

For those exports that do require a license, the typical process for export controls administration and enforcement is depicted in Figure 1.

Figure 1: Simplified Depiction of Export Controls Process

Source: CSIS analysis.

Increasingly sophisticated and well-resourced attempts by Russian and Chinese organizations to evade export controls are not the only reason that BIS's job has become significantly harder in recent years. Legislation and executive orders have posed new challenges to BIS in administering and enforcing export controls in at least three ways.

First, new responsibilities have been added to BIS without additional resources to carry them out. For example, in 2021, the responsibility for regulating and administering exports of firearms moved from the Department of State to the Department of Commerce. However, none of the staff or budget that was performing this function made a move. Similarly, two executive orders during the Trump administration made the Department of Commerce responsible for a broad swath of activities regulating imports of foreign telecommunications equipment, a job ultimately given to BIS. In the Biden administration's Commerce Department budget request for FY 2023, BIS has identified more than $53 million in unfunded requirements from recent legislation and executive orders.

Second, the size of both the Commerce Control List and the lists of parties of concern have expanded significantly. Rising tensions with both Russia and China led the Trump administration and now the Biden administration to expand usage of the entity list. After the full-scale Russian invasion of Ukraine in February 2022, BIS imposed tighter restrictions on exports to Russia. On February 24, 2022, BIS instituted license requirements for exporting controlled commodities to Russia, including all products on the Commerce Control List and Export Control Classification Numbers categories 3–9. This includes goods such as semiconductors, microelectronics, telecommunications, lasers, sensors, navigation equipment, marine equipment, and aircraft components. BIS also expanded the list of entities prohibited from selling and exporting U.S. goods to Russia.

According to the BIS FY 2023 budget request, BIS processed 41,446 license applications in FY 2021. This represents a 9.4 percent increase from FY 2020, when 37,895 applications were processed. Of the 41,446 processed applications, 35,630 (86.0 percent) were approved, 5,109 applications (12.3 percent) were returned without action, and 707 (1.7 percent) were denied. The total value of applications processed and approved in 2020 was $1.3 trillion and $340.5 billion, respectively. Following the release of the two new rules controlling AI semiconductor technology exports to China, BIS estimates that it will need to review at least an additional 1,600 licenses annually.

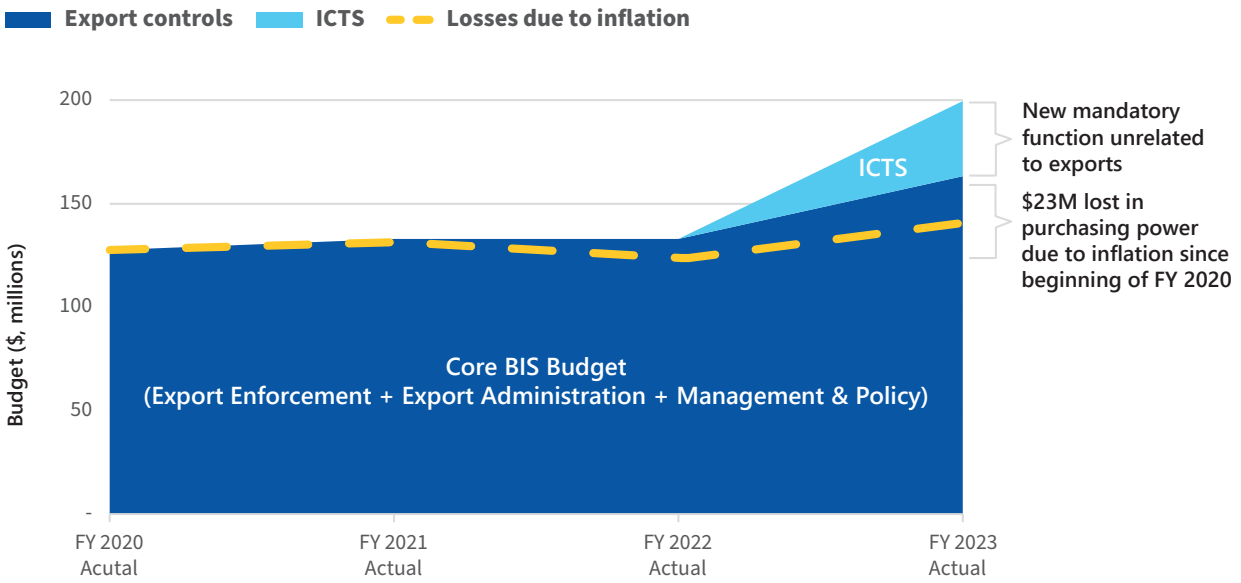
Third, the government has become increasingly creative in creating complex new rules that are often more difficult to administer and enforce. For example, the U.S. approach to export controls has changed significantly via the Foreign Direct Product (FDP) Rule, which consists of an extraterritorial application of U.S. export controls on items manufactured with U.S. equipment, inputs, or design. The application of the FDP rule imposes new license requirements on exports to Russia and China and institutes a presumption of denial policy for license applications for exports or re-exports to Russia and China. The FDP rule is intended to restrict Russia and China's abilities to acquire critical goods such as microelectronics, telecommunications items, and other components with military applications, including from third countries.

The BIS budget for core export control activities has not even kept pace with inflation since FY 2020 and has declined in real terms. The FY 2023 budget request did not address this.

Despite the increased burden on BIS to ensure effective enforcement of export control rules, the increase in available funding for equipping BIS with new licensing and enforcement technology has not increased commensurate with the added enforcement responsibility. The Biden administration's budget submission for FY 2023 does include a request for a $66 million increase in the BIS budget. However, upon further inspection, this budget increase is less than it may seem. A full $36 million of the increase is for a new program called Information and Communication Technologies and Services (ICTS), which is an entirely new and previously unfunded BIS mission focused on policing U.S. imports of foreign technology, such as Huawei telecommunications equipment. An additional $23 million of the BIS budget request should be understood as addressing the loss of purchasing power due to inflation since FY 2020. In short, the demands upon BIS to perform its core function of export controls administration and enforcement have

increased massively since the start of FY 2020, but as of FY 2022, the BIS budget has actually decreased after accounting for inflation (see Figure 2).

Figure 2: BIS Budget Annual Budget by Function



Source: "Fiscal Year 2023: President's Budget Request ," Bureau of Industry and Security, U.S. Department of Commerce, https://www.commerce.gov/sites/default/files/2022-03/FY2023-BIS-Congressional-Budget-Submission.pdf; CSIS analysis.

As shown in Figure 2, even if the Biden administration succeeds in getting its requested budget passed by Congress for FY 2023, nearly 90 percent of the requested $66 million increase will go toward fighting inflation and new missions unrelated to export controls. Furthermore, the request figure was developed prior to Russia's invasion of Ukraine and the new packages of export controls that have been directed toward Russia and China.

In short, the BIS budget is grossly inadequate to keep pace with the changing export control administration and enforcement challenges. This is especially true given the major additional efforts presumably being devoted to export control evasion by Russia and China.

The current state of enabling digital technology for data analysis at BIS is extremely poor. BIS is significantly behind not only the private sector but also other federal agencies.

Across the more than 50 individuals interviewed for this project—including current and former government officials from BIS and other federal agencies, industry executives regulated by BIS, and technology experts—nearly everyone expressed significant concern and frustration over the extremely poor state of BIS's existing technology.

Broadly, there are three sources of data that are needed for BIS to be able to effectively perform its functions across controls list management, license administration, and export control enforcement. These three data sources are (1) internal Commerce Department data; (2) data shared from other government agencies, particularly those involved in trade, law enforcement, and intelligence; and (3) open-source data that is either freely available on the internet or purchasable from private sector data aggregators.

1. **Internal Commerce Data:** Current and former government officials uniformly stated that BIS internal digital infrastructure and databases are in extremely poor shape. For example, the primary government database used for trade transactions contains tens of billions of records. However,

multiple interviewees stated that the system is so unreliable that an identical data search query executed twice in a row will not necessarily retrieve identical records, as various parts of the system are often crashing or otherwise non-responsive. The system's user interface is also complicated and non-intuitive, meaning that new analysts take a long time to become fully proficient in using the system. Moreover, internal Commerce Department data only covers direct U.S. exports and thus has a major gap in monitoring the re-export of U.S. goods from transshipment countries.

2. **Data from Other Federal Agencies:** Representatives from other government agencies, including the intelligence community, stated that BIS's outdated digital infrastructure and tools made it difficult for them to share vital information with BIS and vice versa. In terms of downloading portions of the databases for sharing and more in-depth analysis, BIS analysts generally only have access to outdated versions of Microsoft Excel, a far cry from the more modern knowledge graph and data analytic platforms that have become common among both commercial industry and agencies in government with similar mission requirements as BIS.

3. **Open-Source Data:** However, BIS's greatest deficiencies are arguably in taking advantage of open-source data and data that is available for purchase from the private sector. Government officials requested that CSIS refrain from publishing extensive detail regarding all the open data sources that BIS currently uses or should utilize. This is because governments such as China and Russia that support export control evasion networks have a history of changing their behavior in response to BIS disclosures about sources and methods, as well as from scholarly reports about export controls evasion activity. The authors of this report agree that this caution is warranted. However, it is fair to say that BIS is far too reliant upon public internet search engines and is only taking advantage of a tiny fraction of the open-source data and data analysis capabilities that are available in the private sector. In this regard, BIS is not only significantly behind the private sector but also significantly behind other federal agencies who also have missions where open-source data is useful, such as the Departments of Defense, Homeland Security, and Treasury, as well as intelligence community organizations.

Private sector compliance resources are critical for the viability of U.S. export controls, but they are not a substitute for robust internal capabilities at BIS.

The foundation of the export controls administration and enforcement process is the lists managed by BIS, both the parties of concern lists (e.g., the Entity List) and the Commerce Control List of items. It is the responsibility of BIS to ensure that the lists of parties of concern accurately capture the parties that U.S. law and policy state should be restricted from transactions with U.S. industry. As an industry interviewee said, "if the U.S. government does not want us to do business with an entity, they have to tell us that. They can't just ask us to know that." The same is true for sales of certain types of items. It is the responsibility of the U.S. government to tell industry what is and is not allowed.

As depicted in the simplified process in Figure 1, the export controls process begins with an entity (usually a company) submitting an export license application that provides information about the seller, buyer, and goods or services being sold. A company employee will draft the license application after having made an internal determination about the believed legality of the transaction. BIS holds numerous annual training and informational seminars in order to clarify the existing regulations and policies that companies are subject to. Thus, the most significant resources devoted to export controls are actually performed by private sector entities as part of their compliance and due diligence activities.

However, the primary goals of U.S. companies are generally legal compliance and maximizing profits, not determining and advancing U.S. national security interests beyond what is stated in law and policy. Thus, if the Entity List does a poor job keeping pace with the creation of new Chinese and Russian export control evasion networks, then the considerable private sector resources devoted to corporate compliance will sometimes have only a limited effect on U.S. national security. The degree to which this is the case depends upon the nature of the industry (more consolidated industries are easier to track and control than highly fragmented ones) and on the nature of the goods (large, expensive, and durable items that require significant post-sale servicing are generally easier to track than industries that rely on large-volume sales of inexpensive items).

As mentioned above, recent U.S. policy changes have explicitly acknowledged that BIS's ability to update the Entity List is not keeping pace with the creation of shell companies. As one former U.S. government official told us, the current policy criteria for entity listing imply that "thousands of entities belong on the Entity List but are not there because of lack of resources to do the required analysis." The research and analysis required to put an entity on the Entity List require putting together a robust package of evidence. The package must include not only verified documentation of, for example, the entity's ties to foreign military or intelligence organizations, but also an assessment of the company's technology portfolio, licensing history, and an impact analysis of denying the license that considers the potential for foreign substitution if a U.S. export license is denied. Developing such a package takes weeks or months once BIS has determined that an entity is sufficiently suspicious to deserve an assessment, and there are only a small number of analysts at BIS performing this work. As a result, updates to the Entity List often come years after an entity has already successfully established a shell company to evade an initial entity listing. After an evader's first shell company is discovered and added to the Entity List, the evader merely creates a second shell company.

Since companies are primarily basing their export decisions on compliance with the lists and the regulations that apply to them, this means that no amount of private sector compliance resources and technology can effectively substitute for a BIS that cannot rapidly and effectively update the list.

The primary barriers to improving BIS digital and data infrastructure and the efficacy of export controls are a lack of funding and a lack of staff with the required skill sets.

As mentioned earlier in this paper, BIS funding levels adjusted for inflation have been flat for more than a decade. This reflects the BIS funding and staffing levels that Congress assessed as prudent when the primary focus of national security was terrorism and U.S. military operations in Iraq and Afghanistan. This is no longer the global security environment in which BIS is operating. On October 17, 2022, 10 days after the Commerce Department announced its new export controls policy toward China, Secretary of State Antony Blinken gave a major speech at Stanford University, stating: "We are at an inflection point. The post-Cold War world has come to an end, and there is an intense competition underway to shape what comes next. And at the heart of that competition is technology."

Secretary Blinken is correct. The current era of strategic geopolitical competition is centered around leadership in technology. BIS plays a vital role in ensuring that U.S. technology is not improperly used by foreign governments in ways that are counter to U.S. national security interests. The new export controls policy demonstrates that the Biden administration understands the critical role that BIS must play in this new era.

However, the same cannot be said for the FY 2023 President's Budget request or FY 2022 congressional appropriation. Neither provides adequate resources for BIS to succeed in its vital mission of strategic technology competition.

The simple reason why BIS's enabling technology is in such a sorry state is that the conversation about export controls has been too focused on which items to control at the expense of focus on what it would take for those controls to be effective to the extent required for national security. The U.S. government has provided $18.3 billion in weapons and security assistance funding to Ukraine since Russia's 2022 invasion. While this investment in repelling Russian military aggression is undoubtedly justified, Congress should contemplate how many Russian weapons never would have made it to the battlefield for want of U.S. technology if a tiny fraction of that $18.3 billion had been invested in BIS between 2014 and 2022.

If given adequate funding, BIS could dramatically enhance the productivity and efficacy of export controls by applying modern data science and machine learning technologies.

Improved technology would go a long way toward strengthening BIS's ability to manage its key administrative lists, rapidly assess license applications, and effectively enforce export controls.

BIS enforcement agents engage in open-source intelligence analysis via mainstream search engines and use Excel spreadsheets to comb through data. As one interviewee noted, enforcement officers spend 80 percent of their time looking for data and 20 percent of their time analyzing that data. Creating a system yielding the opposite results—80 percent analysis and 20 percent data gathering—would be far superior. In other words, the use of new technology at BIS would be a major force multiplier. A few noteworthy examples of how modern technology could improve BIS efficacy and efficiency are listed below. These are only a fraction of the total potential.

- Automatic analyst alerting of changes that would affect the validity of previously approved export licenses (e.g., non-Chinese customer entity was acquired by a Chinese company or was identified as a new supplier to the Chinese military)
- A rules-based automatic risk-scoring system for evaluating whether a foreign entity belongs on the lists of parties of concern
- Entity resolution capabilities to establish that different entities are likely related (e.g., automatically detecting that a purported Eastern European "tractor manufacturer" has the same phone number as a known supplier of engines to the Russian military)
- Data provenance tracing and explainable recommendations to ensure that data can be used for law enforcement actions
- Automatically expanding search queries to include translation into other languages, including alternate spellings and adjustments for different data formats
- Allowing for searches based on semantic reasoning in addition to merely keyword matching (e.g., the difference between "X person was witnessed murdering Y" and "X person was a witness to the murder of Y")
- Data fusion into a knowledge graph to allow historically distinct data sets to be cross-referenced and searched with a single interface (e.g., linking U.S. export transactions to likely re-export transactions in third-party countries)
- Transaction monitoring and risk screening
- Identity disambiguation in real time across billions of records

Adopting and leveraging this technology requires several steps. First, it requires harvesting massive open-source data sets. These data sets include but are not limited to corporate executive registries, shareholder registries, property records, tax filings, customs data, shipping and receiving records, vessel ownership data, supply chain disclosures, court filings, government procurement databases, and contract award notifications. One technology expert interviewed for this project said his AI firm is "imagining a world where all public documents are on a map of global documents." For example, while a tractor company may appear to be owned in Eastern Europe, it could use commercial systems to obfuscate illicit business operations. Combing data to understand cross-border associations, shareholders, upstream holdings, and other relevant information—instantaneously—can reveal that the company is owned by an entity in a country of concern and then flag transactions for human review and follow-up.

A second component to leveraging these AI systems is to integrate these open-source data sets with government-restricted ones in a modern data analytics and AI platform. Several government agencies already have technology for the combination of private and open-source data into one database that is updated in real time or near real time. These capabilities can facilitate the rapid identification of supply chain connections to Chinese military end users by reconciling disparate data sources, such as addresses and mutual proximity of specific entities, as well as the specific geolocation of cargo ships, including those that have turned off location-identifying capabilities.

Third, BIS needs to receive this data in machine-readable formats. Several data firms can take large data sets consisting of billions of records and convert them into "knowledge graphs," which structure the relationships and networks between data in a way that is computationally optimized for advanced analysis. Breaking down walls between data sets—for example, a shareholder registry in China and shipping and receiving records in Azerbaijan—can lead the system to generate graphical maps of a possible relationship between these entities and generate red flags that initiate human review.

These tools enhance **entity resolution capabilities**. Entity resolution cross-checks multiple data sources to reference the real world, determining the actual identity of an entity or person. AI systems can analyze billions of records simultaneously by screening identical addresses, overlapping owners, email addresses, social media handles, and other information. These systems can also account for flipped dates of birth and misspelled addresses, which can be difficult for humans to catch. Furthermore, these AI systems can operate in a host of languages, including Burmese and Mandarin.

The private sector already uses a wide array of technological capabilities to ensure compliance. Scanning tools are common in the financial services sector, for example, which conducts automated scans of billions of records to detect fraud. It is unreasonable to assume that a financial institution would have humans comb through these records in real time or expect results to satisfy consumer demand for satisfactory fraud prevention.

However, in technology that BIS would adopt, technology providers tend not to "score" the data. In other words, the external technology and data providers do not effectively determine whether export control evasion is occurring; they flag suspicious activity for human review and leave it to the government to take action based on a review of the data. As one AI expert explained in an interview with CSIS, "an algorithm can tell you where the risks are. From there, a group of people can investigate these risks closely. Then you can point back to the entire data provenance and justify how you got to the end result." One of the key benefits of using an AI-based system is that it allows disparate data sources to be woven together instantaneously, vastly increasing the enforcement and investigation capabilities of BIS officers.

As the enforcement picture changes and the need to identify and prevent Russian circumvention accelerates, existing technology offers the U.S. government an opportunity to adopt new data-mining tools

that would considerably expand enforcement capabilities. The adoption and use of this new technology offer dramatic benefits. These include:

1. **Substantial Analyst Productivity Increases:** The adoption of new technology could flip the search versus analysis equation, significantly streamlining workflows and enforcement capabilities by shifting time spent searching for data to analysis of data.
2. **Swifter Identification of Circumvention:** Automated systems can comb through billions of documents and information sets simultaneously, generating real-time red flags.
3. **Digitized Auditable Systems:** An auditable system provides a traceable evidence trail that can justify any subsequent enforcement action and can be upheld in court.
4. **Potential to Reduce the Regulatory Burden:** In 2021, BIS took 26 days on average to issue licenses. The adoption of new technology would speed up licensing processes and reduce compliance costs over time.
5. **Amplified Enforcement Capabilities:** The combination of new enforcement technology with existing human resources at BIS would dramatically enhance overall export control enforcement capacity at BIS.

Digitizing licensing and enforcement would increase productivity, reduce private sector burdens, and directly impact the Russian war machine by allowing the real-time cross-checking of large data sets, such as the interagency Automated Export System (AES), against BIS's internal system, classified intelligence, and open-source intelligence.

Evidence from comparable organizations suggests that Congress should appropriate no less than $25 million annually for the next five years for BIS technology modernization.

Based on discussions with members of the U.S. trade, law enforcement, and intelligence communities, as well as private sector technology providers, Congress should allocate $25 million of funding to BIS annually in addition to the initial system buildout, updates, training, and maintenance. It will require continued support for years to come, particularly if the export control enforcement environment becomes substantially more complex in the future.

An appropriation of $25 million annually for the next five years will help significantly enhance immediate enforcement capabilities and also improve the speed and accuracy of export licensing. This figure takes into account BIS's opportunities to improve collaboration with other U.S. government agencies and the need to prevent unnecessary duplication of effort. This funding will go toward four primary areas: (1) procuring access to large proprietary and open-source data sets, (2) integrating those data sets into a modern data analytics platform, (3) adding additional analyst staff with needed specialist skills to use new technology (e.g., data scientists), and (4) covering staff training costs. Specifically, this funding should support the following mission objectives:

- Adopt a more proactive rather than reactive approach to export controls
- Leverage a new technology suite to provide real-time data about export control evasion
- Expand the analyst staff and train BIS staff with relevant courses

For ensuing appropriations, it is important that Congress provide sufficient funding to enable BIS and its data contractors to keep the source code and inputs evergreen, which will necessitate frequent updating and

monitoring. Although the adoption of this technology will also have significant cost-saving effects on staff time and bandwidth, the initial bucket of funding will be needed to train BIS staff to use the new technology.

Overall, BIS needs an integrated solution that takes inputs from multiple private sector data vendors, integrates them into a unified data platform (on government networks or government clouds), performs relevant analytics on the data, and presents that in a usable user interface for government analysts. Obtaining large data sets such as the ones discussed above is one of the costly elements in standing up a digitized enforcement system. An additional cost involves the disambiguation of data into a readable format, which represents a separate added cost.

In addition to acquiring the rote data, a core cost will be for BIS to work with external technology providers and contractors to ensure that the data is searchable and readable, enabling BIS staff to maximize the benefits of the technology. Another cost relates to staff training. One interviewee for this project noted that the training involved for export enforcement staff would be minimal, estimating that someone could learn how to use a new AI system in a matter of hours. However, full utilization of enforcement technology could vary significantly depending on the technological acuity of staff, so BIS will need to hire more specialists and provide additional training to existing staff.

Additional funds appropriated by Congress will allow BIS to leverage existing and externally available technology to support its licensing and enforcement needs. In addition to acquiring the rote data, a core cost will be for BIS to work with external technology providers and contractors to ensure that the data is searchable and readable, enabling BIS staff to maximize the benefits of the technology. Experts building comparable systems for the intelligence community and other federal agencies with similar missions to build, maintain, and staff this technology stack would cost roughly $25 million annually.

Procuring technology is only part of the solution. Congress needs to appropriate funds on an annual basis to ensure that BIS staff are able to leverage the technology. Furthermore, funding extra staff will help close ongoing gaps in enforcement, particularly as enforcement needs grow in number and complexity. In other words, simply acquiring new technologies is not a panacea on its own; successful use of new technologies depends on the agency's ability to use them effectively.

In addition to the $25 million for technology modernization and analyst staff, Congress should provide $18.4 million in annual funding for additional enforcement agents.

Notably, many individuals said that while new technology could radically improve the productivity of the export administration and enforcement analytic communities, additional resources are likely needed for other parts of the BIS export enforcement enterprise. This is because a more productive enforcement analysis community will identify more entities as likely shell companies engaging in illicit transactions. This will in turn increase the need for enforcement agents to conduct site inspections or criminal investigations of these identified entities. Despite the severe current technological limitations on the efficacy of the analytic community, its work is already identifying enough candidate entities for inspection to more than fully consume the capacity of the current staff.

The current criminal investigator cadre is spread too thin to counter threats to U.S. national security. It is routine for a single BIS ECO to be responsible for working with multiple foreign countries or entire regions. Within the United States, many BIS agents have extremely high caseloads with responsibility for conducting far more investigations than they can effectively handle. As one interviewee put it, "even if BIS had 500 domestic criminal investigators, they would be overwhelmed with full time work."

As a result, in addition to the funding for new technology, BIS will also need additional enforcement agents and funding with which to pay them. Therefore, in addition to the $25 million annual increase for five years to support new technology and staff for BIS analytical capabilities, BIS will also require an additional $18.4 million and 48 positions annually for the Office of Export Enforcement. BIS would also require $1.2 million for additional sensitive compartmented information facility (SCIF) space to support the classified aspects of this program for an overall total of roughly $19.6 million. Therefore, the total size of the recommended additional budget appropriation is $44.6 million annually.

Providing additional funding, staff, and technology capabilities for BIS is a win-win opportunity with a high return on investment for both U.S. exporters and the U.S. government.

While the relatively small staff at BIS has demonstrated its admirable ability to take on a task of massive economic and national security proportions, the adoption of a new data-driven technology stack could substantially increase export enforcement capabilities. Given the dramatically expanded 2022 Russia export controls, the changing geopolitical landscape with China and Taiwan, and increasingly sophisticated smuggling networks, the need for BIS to adopt new data-driven digital technologies for its enforcement efforts is both clear and urgent.

The evolving geopolitical threat landscape presents Congress with a historic opportunity to couple its support of Ukraine and its defense of democracy with new technological capabilities that are more effective in identifying circumvention of export controls and which also contribute to the long-term degradation of a potential military adversary.

Compared to the annual $44.6 million cost, the benefits of this investment in BIS are extremely attractive. The U.S. government is currently spending tens of billions to assist Ukraine in destroying the weapons of Russia's military, which too often are powered by U.S. technology. Providing a few tens of millions of dollars annually to BIS to modernize the technology that enables effective export controls would go a long way toward ensuring that far fewer Russian and Chinese weapons using U.S. technology are built in the future. The disparity between the meager cost and the massive opportunity is so great that this likely represents one of the opportunities with the highest return on investment available anywhere in U.S. national security. ■

Gregory C. Allen *is the director of the Artificial Intelligence (AI) Governance Project and a senior fellow in the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C.* ***Emily Benson*** *is a senior fellow with the Scholl Chair in International Business at CSIS.* ***William Alan Reinsch*** *is a senior adviser and holds the Scholl Chair in International Business at CSIS.*

The authors would like to thank CSIS interns Elizabeth Duncan and Daniel Elizalde for their thoughtful input and research assistance.

This report was made possible through generous support from Schmidt Futures and Accrete AI.