Bureau of Industry and Security 2022 Agenda

Recommendation #1:

Strengthening Enforcement to Detect, Identify and Deter Export Control Violation

FUTURE OF BIS

www.futureofbis.com

The Department of Commerce's Bureau of Industry and Security (BIS) is probably the most important U.S. government agency most have never heard of. Charged with ensuring export control, treaty compliance, and strategic technology leadership, BIS plays a critical role in U.S.-China policy and without its due diligence, American-made, sensitive and strategic technologies could end up in the hands of the Chinese military and threaten America's national security.

President Biden has nominated Alan Estevez for Under Secretary of BIS, Matthew Axelrod for Assistant Secretary of Export Enforcement, and Thea Kendler to serve as Assistant Secretary for Export Administration in the U.S. Department of Commerce. The nominees bring unparalleled national security experience to BIS at one of the most critical junctures in the agency's history. This series of policy recommendations will provide ideas for BIS and its leadership to pursue an aggressive agenda and use the agency's full range of tools to protect America's security and prosperity.

The purpose of U.S. export controls is to "enable BIS to address threats to the national security and foreign policy interests of the United States while bolstering continued U.S. industrial competitiveness and innovation." Export controls protect security by ensuring that dual-use technologies are not weaponized against Americans, and they protect prosperity by ensuring that strategic technologies are not acquired by adversaries.

According to the agency's 2020 Annual Report, BIS investigations produced 36 criminal convictions last year for export control violations. This resulted in just more than $2,141,000 of combined restitutions, forfeitures and fines and 615 months of imprisonment—or less than $60,000 of financial penalties and 15 months of jail time, on average.

While these statistics show an increase in BIS enforcements over prior years, the levelof enforcement is still low compared to the total value of export of dual-use technologies. The export of goods which can be used for commercial and military purposes exceeds tens, if not hundreds of billions of dollars, annually. With roughly 100 enforcement officers, BIS can review only a small fraction of all sensitive exports. Moreover, BIS has the capability to fine violations at double the value of the transaction. This white paper briefly explores enhancing BIS enforcement through workforce and penalty optimization.

SETTING THE BASELINE FOR EFFECTIVE ENFORCEMENT

Evaluating BIS' capability to detect, identify, and deter export control violations is important for policymakers. BIS is housed within the larger U.S. Department of Commerce with a $10 billion annual budget and more than 46,000 employees. However BIS itself, a recognized critical agency for national security, has an annual budget of approximately $122 million and 450 full-time employees with roughly one-quarter engaged in enforcement. The policy research question is to what degree BIS fulfills the enforcement function among its other priorities, which include tasks such as managing the Entity List.

Setting a baseline is difficult as there is limited data; it is not known how many violations are undetected and whether they are significant. More largely, it is difficult to compare U.S. export control enforcement to other countries because most do not allow the publication of civil export control enforcement actions. However, Kevin Wolf, former Assistant Secretary of Commerce for Export Administration, says the United States "by far exceeds all other countries combined." Wolf, now in private practice, argues in testimony to the Senate Banking Committee for greater resources for enforcement to improve fairness for the many companies which endeavor to comply with BIS regulation. The larger argument for strategic trade control is that it expands the playing field for legitimate, lawful trade.

Dual-use items are commodities, software, or technology with both commercial and military uses including semiconductors, navigation systems, radio frequency modules, and smoke bombs among thousands of other items. Through the Wassenaar Arrangement, 42 nations including the U.S., agree on the dual-use items to be controlled, but there is little international coordination on the enforcement of these controls. In any event, there is general recognition in the U.S. that enforcement is important, particularly with trade with the People's Republic of China (PRC) and ensuring that dual-use items do not make their way to military end users or uses. Notably BIS refers criminal cases involving theft, smuggling, and other crimes to the Department of Justice for prosecution. This underscores that export controls are one important element of security, but alone are insufficient to address the complex military challenge of the PRC.

BIS provides valuable insight in its 2020 document summarizing 150 actual investigations of export violations in the nuclear, bio-chemical, and missile tech domains; the practices of some terrorists and freight forwarders, the workaround of parties attempting to avoid boycotts, and crimes by sundry exporters. This suggests that violations are real, significant, and worthy of additional policy attention.

IMPROVING THE EFFECTIVENESS OF BIS ENFORCEMENT: PENALTIES

BIS's Office of Export Enforcement (OEE) assesses penalties for export control violations. The structure of these penalties, updated in 2016, models the Treasury Department's Office of Foreign Assets Control (OFAC) and were designed to improve the transparency of fines. The amounts of the penalties were codified as part of the Export Control and Reform Act of 2018 (ECRA), a major reform to the agency. For comparison in 2020, OFAC issued 17 enforcement actions with $23.6 million in penalties, compared to 2019 with the 30 enforcement actions and almost $1.3 billion in penalties. The reduced totals in 2020 likely reflects the pandemic and fewer cases. 2019 was animated by a $657 million penalty against Standard Chartered in 2019 and 2017 by the $100 million settlement with ZTE, significantly reduced from the first iteration of $1 billion, a combined BIS and OFAC penalty.

The OEE weighs the seriousness of violations based on a set of "aggravating factors," whichinclude willfulness, recklessness or gross negligence, concealment, pattern of conduct, prior notice, and management involvement. A monetary penalty may be applied if the OEEdetermines a violation to be "egregious," in which case the base fine can be "up to one- half of the statutory maximum penalty (capped at $125,000)" if self-reported and as much as double the statutory maximum (capped at $284,582) if the "apparent violation comes toOEE's attention by means other than a voluntary self-disclosure."

Maximum criminal penalties for willful violations are $1 million and up to 20 years in prison for individuals. Maximum civil penalties are $300,000 or twice the value of the applicable transaction, whichever is greater.

Notably the total fine can reflect multiple violations within a transaction and the value of the transaction itself. The BIS penalty regime encourages voluntary self-disclosure (VSD), the notion that firms, which have violated the export regime, can disclose the violation and potentially receive a 50 percent reduction on their penalty.

Updating the penalty regime included an important debate about the structure and level of fines. For example, the maximum fine could be equal to double the dollar value of the transaction. Some find this high while others suggest it is too low. Many dual-use items may have a low dollar value but can inflict a high level of damage when deployed in military use.

Importantly, when considering this debate, understand these export control civil penalties should not be confused with the criminal penalties defined by law and administered by the Department of Justice.

WORKFORCE: THE PEOPLE AND TOOLS FOR A SPECIAL TASK

Export control compliance is a highly specialized form of law enforcement which involves the knowledge and expertise in dual-use products, civil and criminal investigations, the practices of sophisticated exporters, and the behavior of furtive end users. This function may well be improved with technology and tools for tracking and targeting and coordination with other law enforcement agencies such as Federal Bureau of Investigation, Department of Defense, and the Department of Homeland Security. Many career officers and agents developed highly specialized skills following 9/11 and the workings of terrorists.

As the PRC has emerged as the leading threat to the U.S., an enhanced set of tools and skills is likely required to detect, identify, prosecute, penalize and deter violations. The PRC has demonstrated its ability to obscure military users and uses. Advanced U.S. technology is highly valued in the PRC, and many U.S. firms have earned record profits selling this technology, even when it could potentially put Americans' security at risk. BIS enforcement officers require intelligence and integrity to navigate this field. Their day-to-day tasks include intercepting illegal exports, conducting checks, monitoring users and uses, educating exporters on compliance, and pursuing violators.

An important area for further research is whether the roughly 125 agents is sufficient for the task. Half a dozen BIS officers are posted abroad where they could review sensitive exports on the ground. Some suggest that, at a minimum, the number of total special agents should be doubled. One way to manage that evolution could be to stagger the addition of agents with a corresponding evaluation of the number and type of violations detected. As the violations increase, agents could be added accordingly. Additionally, investment in tools and tactics such as audits, statistical modeling, algorithmic and artificial intelligence analysis could be explored for better detection, identification, and deterrence. U.S. industry could explore legitimately improving and promoting their BIS compliance, ideally in concert with other like-minded nations and their countries' firms.

Congressional resistance to increasing BIS budget and headcount could be related to other issues such as overall financial constraints of the U.S. government and other policy matters such as the debate on the list of emerging and foundational technologies required by ECRA, a topic to be covered in a future China Tech Threat white paper.

CONCLUSION

Maintaining the United States' advantage in key technologies is critical to national and economic security. Export controls provide one of the few frontline defenses to stop adversaries like the PRC from gaining U.S. technology. It is not clear how many export control violations the U.S. may be missing and to what degree the BIS enforcement workforce and penalties as applied are optimal. BIS has significant leeway to increase penalties, up to twice the value of applicable transaction. The number, skills, and tools of enforcement officers should also be evaluated. These should be among the priorities for the next BIS Undersecretary to ensure that export control violations are detected, identified, and deterred.