Fact Sheet: Transforming the Bureau of Industry and Security Under the Leadership of the Biden-Harris Administration

Over the last four years, the United States has faced an increasingly dynamic threat environment. Malign actors like the People's Republic of China (PRC), Russia, the Democratic People's Republic of Korea (DPRK), and Iran have grown more sophisticated and assertive. Additionally, advancements in dual-use critical technologies like artificial intelligence (AI), semiconductors, and biotechnology have transformed the way we innovate and have the capability to change how we conduct warfare. These commercially available advanced technologies are now central to U.S. national security.

To meet this challenge, the Department of Commerce has taken on a more robust role in advancing our national security through *offense* – making key investments in U.S. technology and manufacturing leadership – and *defense*, by ensuring our adversaries are unable to procure technologies that can be used for military advancement, including the development of advanced AI capabilities, advanced weapons systems, and other applications that may threaten the national security of the United States.

Under the leadership of Under Secretary Alan Estevez, the Bureau of Industry and Security (BIS) has become central to the U.S. government's national security strategy. Throughout the Biden-Harris administration, BIS has revitalized its approach to controlling technology, taking unprecedented actions to prevent adversaries from accessing advanced U.S. and allied technologies and working to bring other countries into a U.S.-led trusted technology ecosystem. BIS has also transformed as an organization, leveraging new tools and authorities to counter adversaries who pose threats to our technology supply chains and defense industrial base.

Among other accomplishments, BIS has:

- Imposed proactive and sweeping sector and country-wide export controls to impede the PRC's ability to access and indigenize production of advanced semiconductors and related items, which can be used to develop advanced AI capabilities and weapons systems;
- Established the Office of Information and Communications Technology and Services (OICTS) – the Bureau's third and newest component – in 2022 to address foreign adversary threats to critical infrastructure supply chains. Since then, Commerce issued the program's first Final Determination in an individual investigation in 2024 (banning sales of Kaspersky Labs products); finalized the program's groundbreaking, first-ever class-based regulation of the import or sale of connected vehicles and related technologies with a nexus to the PRC or Russia; and significantly increased OICTS hiring;

- Created and built powerful international coalitions and partnerships to address foreign adversary procurement of critical technologies, including those related to quantum computing, semiconductors, and additive manufacturing, and imposed sweeping export controls against Russia following its unprovoked invasion of Ukraine in 2022; and
- Launched the Disruptive Technology Strike Force, co-led by the Department of Justice, to protect advanced technologies from illegal acquisition by foreign adversaries like Russia, the PRC, and Iran.

BIS has focused its efforts on four key pillars:

1. Impeding PRC technology and military modernization;
2. Degrading Russia's military industrial base;
3. Protecting U.S. technology and related supply chains; and
4. Strengthening coordination with our allies and partners.

1. Impeding PRC military modernization

BIS has spearheaded the Biden-Harris administration's efforts to restrict the PRC from accessing sensitive U.S. technologies. Under a "small yard, high fence" approach, BIS aimed to control only items necessary for the PRC's military modernization, which could be used to develop advanced weapons systems and AI capabilities.

- *Major Semiconductor Rules:* BIS has implemented groundbreaking and surgical restrictions on advanced semiconductor technology exports to China, controlling not only advanced chips but also the equipment needed to make them, through three major semiconductor packages in October 2022, October 2023, and December 2024. As a result, the PRC maintains limited advanced chipmaking capabilities – more than 5 years behind the current leading edge.
    - *October 2022*: BIS imposed new controls to restrict the PRC's ability to purchase and manufacture certain high-end chips critical for military advantage.
    - *October 2023*: The following year, BIS strengthened the parameters of advanced chip controls and enhanced controls on chip manufacturing equipment and items to other destinations of concern beyond the PRC.
    - *December 2024*: BIS introduced significant new controls on semiconductor manufacturing equipment, software tools for developing or producing advanced semiconductors, and first-of-its-kind controls on high-bandwidth memory (HBM) – used in almost all AI data center chips. The package also included several changes to enhance the effectiveness of our controls, including new red flag guidance addressing compliance and diversion

concerns, and new Entity List additions spanning PRC tool manufacturers, semiconductor fabs, and investment companies involved in furthering PRC military modernization. In January 2025, BIS also strengthened its controls to enhance due diligence by foundries and improve safeguards against diversion to the PRC and other entities.

- *Entity Listings:* BIS added over 55% (nearly 600) of the over one thousand PRC entities on the Entity List under the Biden-Harris administration, including over 300 in 2024. We have more than doubled the number of PRC entities on the Entity List during the last four years.
- *Enforcement Actions:* BIS's Export Enforcement component imposed its largest-ever standalone administrative penalty – $300 million – against a company for violating our export controls by shipping millions of hard disk drives to Huawei that were manufactured abroad but produced using U.S. technology, and brought numerous enforcement actions against Chinese procurement networks.

2. Degrading Russia's military industrial base and capacity to wage war

After Russia's unprovoked invasion of Ukraine in February of 2022, BIS demonstrated unwavering commitment to addressing Russia's illegal actions. The Biden-Harris administration's policies have damaged Russia's supply chain and forced Russia to contend with the rising costs of establishing and re-establishing illicit procurement networks to avoid our controls. Russia now finds it increasingly difficult to procure sensitive microelectronics made by U.S. and allied countries, and as a result of U.S. export controls, Russia has been forced to pay more for microelectronics and critical tools to sustain their military industrial base.

- *Regulatory Actions*: BIS published nearly 50 rules imposing a range of restrictions on Russia and its enablers in Belarus, Iran, and the PRC. These rules imposed controls on an unprecedented number of items, including 2,500 lower-level technologies.
- *Multilateral Action:* BIS led the implementation of a Global Export Control Coalition (GECC) to impose stringent export controls on Russia and Belarus in concert with 38 partner countries. This group continues to share critical information and coordinate controls on Russia, resulting in the restriction of thousands of items to Russia and a significant decrease in the production and procurement of items that feed Russia's defense industrial base.
- *Entity Listings*: BIS added more than 65% (over 750) of the over one thousand Russian entities currently on the Entity List, including over 500 since Russia's invasion of Ukraine in 2022. BIS also began to use the Entity List in an innovative new way to address diversion and transshipment to Russia, surgically targeting

addresses of Hong Kong corporate secretaries, shell companies, and locations with multiple targets, more effectively constraining Russia's global procurement networks.

- *Enforcement Actions:* Completed a record number of Temporary Denial Orders, detentions, and end-use checks to identify and prevent the diversion of U.S. items to Russia, as well as announced significant criminal and administrative enforcement actions. These included 100 indictments, 49 arrests, 12 extraditions, and 21 sentences related to the unlawful transfer of sensitive information, goods, and military-grade technology to Russia. BIS also issued 19 administrative and denial orders, including violations involving Common High Priority List items, which Russia specifically seeks to procure for its defense industrial base to support weapons programs used in its full-scale invasion of Ukraine.
- *Industry Engagement:* BIS, along with teams from the Department of State and the Department of the Treasury, led a comprehensive effort to engage the leadership of U.S. microelectronics companies to better mitigate the diversion and transshipment of high priority microelectronics and components to Russia and third countries. BIS also led an effort to engage Canada, France, Germany, Italy, Japan, the United Kingdom, the United States; the European Union (EU), the Republic of Korea, and Australia (The G7+) on similar industry outreach in their respective countries. BIS's engagement efforts also included issuing an unprecedented 11 guidance documents, including in coordination with interagency and international partners, on preventing diversion to Russia.

3. Protecting U.S. technology and supply chains

For decades, BIS has focused on slowing the proliferation of dual-use military items and nuclear, chemical, and biological weapons, as well as preventing U.S. technologies from being used to commit human rights abuses by malign actors through effective export control and export enforcement regimes. Under the Biden-Harris administration, BIS has expanded its role through the establishment of the Office of Information and Communications Technology and Services (OICTS) – its third and newest component, dedicated to securing our supply chains from foreign malign intervention – and worked to create guardrails around sensitive technologies like AI.

- *Securing Connected Vehicles*: In January 2025, after a robust regulatory process, OICTS issued a final rule to prohibit connected vehicles – and certain connected vehicle technologies – linked to foreign adversaries from being imported into or sold in the United States. This first-of-its-kind final rule secures connected vehicle supply chains from foreign adversary threats, limiting the PRC and Russia from gaining access to the sensitive information our cars collect and manipulating vehicles on American roads.

- *Kaspersky Labs Final Determination*: In June 2024, OICTS prohibited the sale and distribution of Kaspersky Lab's antivirus software within the United States through its first-ever Final Determination. Kaspersky's ties to the Russian government posed a significant national security risk for Americans purchasing or using its software. The company has since begun to cease all operations in the United States.
- *Safeguarding Commercial Drones*: In January 2025, OICTS published an Advance Notice of Proposed Rulemaking requesting public comment to better scope potential actions addressing foreign adversary threats to the supply chain of commercial unmanned aerial systems (UAS), or drones.
- *Responsible AI Framework:* Under the Biden-Harris administration, BIS released several major regulations to promote American innovation in AI while protecting national security. These included an expansion of the Validated End User (VEU) program to include AI data centers, followed by a larger responsible AI framework to help build a trusted technology ecosystem around the world while ensuring countries of concern are restricted from accessing the most advanced AI chips and closed frontier model weights.
- *Addressing Biotechnology Risks*: In January 2025, BIS instituted new controls on certain dual-use laboratory instruments, including high-parameter and spectral flow cytometers and cell sorters and certain liquid chromatography mass spectrometers (LC/MS), that could be exploited by foreign adversaries to further their military capabilities and threaten U.S. national security.
- *Enforcement Actions:* BIS Export Enforcement made several fundamental changes under the Biden-Harris administration to better enforce export controls and protect American technology, including establishing the Commerce Screening System to automate the screening of foreign entities on export license applications against intelligence holdings; publicly releasing charging letters when filed; publishing lists of the names of parties making boycott requests; raising penalty amounts for serious violations; and enhancing BIS' voluntary self-disclosure policy.

4. Strengthening coordination with allies, partners, and other stakeholders

Export controls are most effective when they're multilateral. Under the Biden-Harris administration, BIS has strengthened its relationship with a range of allies and partners abroad as well as stakeholders at home, and launched innovative partnerships to secure critical technologies from foreign adversaries.

- *Multilateral Export Enforcement*: BIS established the Disruptive Technology Protection Network with Japan and South Korea to expand information-sharing and share enforcement best practices; established innovative new export

enforcement coordination mechanisms with the G7; and launched the Export Enforcement Five (with Australia, Canada, New Zealand, and the United Kingdom) to enhance international enforcement coordination.

- *AUKUS Partnerships*: BIS streamlined trade in dual-use items with AUKUS (a trilateral security partnership between Australia, the United Kingdom, and the United States) by removing license requirements for the export/reexport to the United Kingdom and Australia of several categories of items, including munitions, missile technology, and hot section engine technologies; increasing the availability of license exceptions for reexport; and removing restrictions on the export of high-speed and thermal imaging cameras to armed forces or for the production of military equipment. BIS also expanded license-free treatment to include certain space-related exports, no longer requiring a license for the export of certain remote sensing or space-based logistics, assembly, and servicing satellites/spacecraft to some of our closest allies.
- *Plurilateral Controls on Sensitive Technologies:* BIS published new controls on quantum computing, strengthening our trade and diplomatic relationships by creating a carveout for like-minded countries that institute similar controls. Additionally, BIS has engaged in comprehensive discussions and negotiations with allies and partners to mitigate diversion risks as well as to ensure our adversaries are unable to backfill export-controlled items, addressing the risk of advanced technology being acquired for interests counter to U.S. national security.
- *Enforcement Efforts:* Launched a robust and unprecedented enforcement effort with interagency partners through the Disruptive Technology Strike force, resulting in the highest number ever of convictions, months of imprisonment, temporary denial orders (TDOs), post-conviction denial orders, and the highest standalone administrative penalty in BIS history. Since its inception, the Strike Force has publicly charged 26 criminal cases, a 50% increase in criminal enforcement actions compared to the two years before its inception.
- *Academic Outreach*: BIS implemented an Academic Outreach Initiative with 40 American research institutions to help universities protect their sensitive research from nation-state adversaries who seek to acquire it.