Steptoe

Steptoe White Paper: Artificial Intelligence and the Landscape of US National Security Law

JULY 2024

Table of contents

Table of contents cont'd

Introduction

This white paper is intended to provide a broad overview of the various US national security laws that can apply to AI, illustrating the breadth of legal regimes that AI companies and companies using AI must keep in mind and the complexity of applying many of these regimes to novel developments in this rapidly evolving space.[1]

Much of today's discussion on AI centers around the lack of laws and regulations and the need for policymakers to catch up to rapidly evolving industry developments. Despite this narrative, AI is already subject to a significant number of national security-related laws and several new legal regimes will be implemented in short order. These national security-related regimes can apply to obvious cases such as the use of AI in weapons systems, but can also apply to AI with no clear, direct connection to national security. AI systems used in critical infrastructure, AI algorithms that power social media feeds, and generative AI that can create so-called "deepfakes" are just a few examples of AI systems that may implicate a number of US national security laws.

While US policymakers are concerned about strategic competition with a number of foreign rivals and adversaries, there is no doubt that China is the country of greatest concern to US officials with respect to AI and national security. Of the various legal regimes and provisions discussed in this white paper, some are laws of general applicability applying regardless of jurisdiction, some target a handful of jurisdictions viewed by US officials as particularly problematic, and some target a single country such as certain export controls measures against China or Russia.

Certain laws discussed herein apply broadly to transactions or other dealings that implicate US national security, generally, while others apply specifically to AI. AI systems rely on two fundamental building blocks: (1) advanced semiconductors needed to provide sufficient computing power to train, and in some cases operate, AI models and (2) significant quantities of data used to train AI models. Both of those building blocks are also subject to a range of US national security laws and, while this paper focuses on AI software, it will also touch on those elements.

1 For purposes of this white paper, "AI companies" include companies developing, testing, training, researching, and selling or distributing AI products and services. "Companies using AI" refers to non-AI companies that use AI developed by others as part of their products and services. Given the rapid evolution of AI, and accompanying legal and regulatory frameworks, we anticipate updating this white paper periodically.

I. Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

While many US national security laws already apply to AI, we begin with a discussion of the new national security regimes that will be implemented in the near future.

On October 30, 2023, President Biden issued an *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (the "AI EO").[2] The preamble to the AI EO explains that the Biden administration "places the highest urgency on governing the development and use of AI safely and responsibly, and is therefore advancing a coordinated, Federal Government-wide approach to doing so."[3] It adds, "The rapid speed at which AI capabilities are advancing compels the United States to lead in this moment for the sake of our security, economy, and society."[4]

Although the AI EO touches on a number of areas, perhaps the most significant and detailed area of the AI EO is Section 4 entitled "Ensuring the Safety and Security of AI Technology," which lays out a number of key policy priorities related to AI and national security. Below we lay out some of the key initiatives from Section 4 of the AI EO.

A. Development of new standards, tools, and tests

The order requires the Department of Commerce (Commerce), including the National Institute of Standards and Technology (NIST), and other federal agencies, to establish guidelines and best practices to promote "consensus industry standards for developing and deploying safe, secure, and trustworthy AI systems."[5] This includes creating or revising existing standards related to AI risk management, secure software development, evaluating and auditing AI capabilities, and red-teaming.[6] These standards cover a wide range of areas, including dual-use foundation models;[7] generative AI; use of AI in critical infrastructure; so-called "synthetic content," including deepfakes; and nuclear, chemical, radiological, and biological weapons proliferation, among many other topics.

While many of these standards are intended to be voluntary, others are intended to form mandatory requirements and certain of the voluntary standards could become mandatory with time – either because industry expectations make them a *de facto* requirement or because they are embedded in future regulations, statutes, or contracts with the US government.

Some of these standards have been released, at least in draft form, and are discussed below, while others are forthcoming.

B. Rules for developers of powerful AI models to share information with the us government

The AI EO directs the Department of Commerce to issue regulations requiring companies "developing or demonstrating an intent to develop potential dual-use foundation models" to provide regular reports to Commerce on a variety of topics, including: current and future business activities related to training, developing, and producing dual-use foundation models; the ownership, possession, and protection of the model weights of the dual-use foundation model; and the results of red-team testing based on guidance from the Department of Commerce and NIST, among other topics.

The order also mandates the promulgation of rules requiring reporting by persons that "acquire, develop, or possess a potential large-scale computing cluster," including "the existence and location of these clusters and the amount of total computing power available in each cluster."[8]

2 "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," 88 FR 75191 (Oct. 30, 2023), https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence

3 *Id.*

4 *Id.*

5 Exec. Order No. 14110, § 4.1(a)(i).

6 As defined in the AI EO, the term "AI red-teaming" means "a structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI." Exec. Order No. 14110, § 3(d).

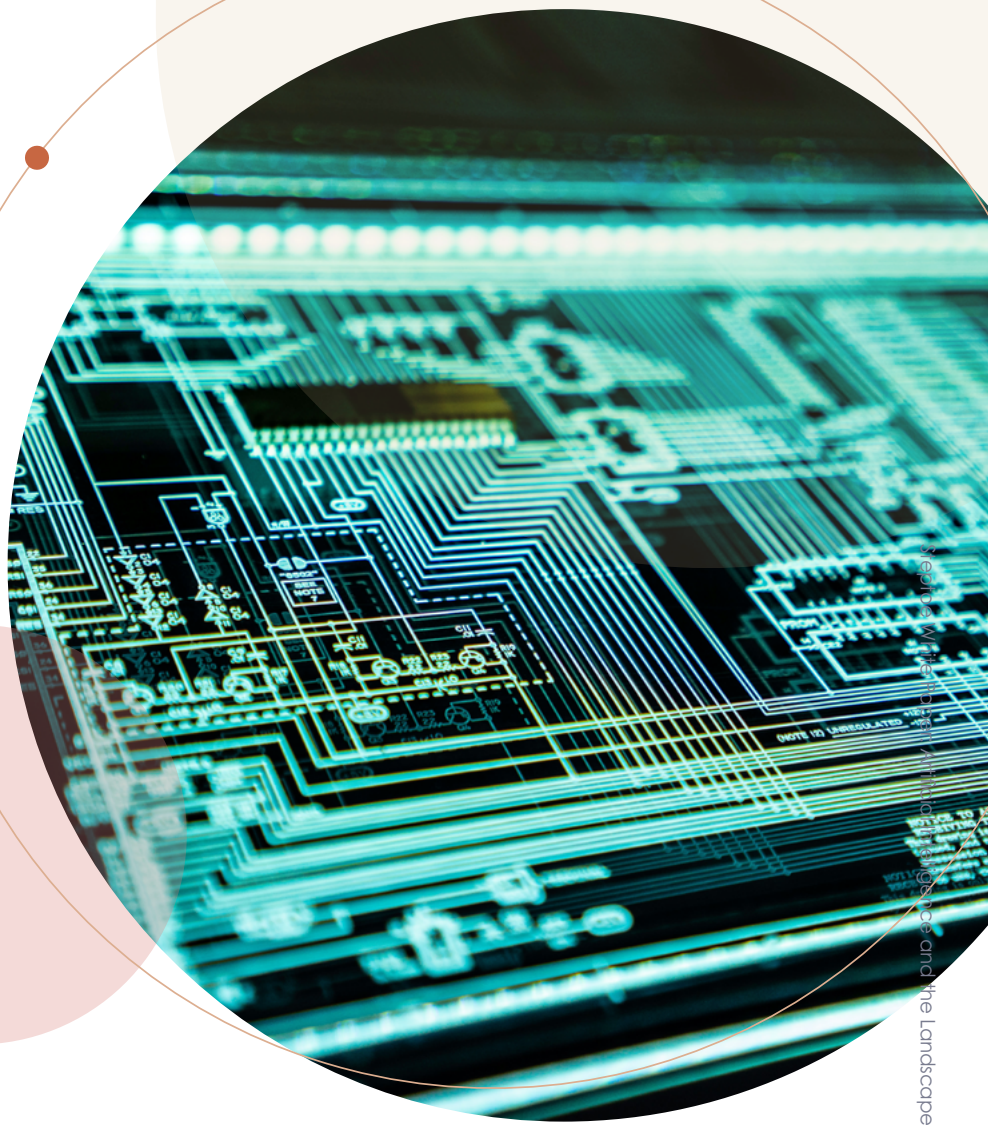
7 The AI EO defines a "dual-use foundation model" as "an AI model that is trained on broad data; generally uses self-supervision; contains at least tens of billions of parameters; is applicable across a wide range of contexts; and that exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety, or any combination of those matters…." Exec. Order No. 14110, § 3(k). Notably, models fall into the above parameters "even if they are provided to end users with technical safeguards that attempt to prevent users from taking advantage of the relevant unsafe capabilities." *Id.*

8 *Id.*

C. Reporting and customer due diligence rules for iaas providers

With respect to infrastructure as a service (IaaS), the AI EO directs the Department of Commerce to require IaaS Providers to report to Commerce "when a foreign person transacts with that United States IaaS Provider to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity."[9] Such reporting obligations must also be flowed down to "foreign resellers" of the IaaS Product.

The order further directs Commerce to issue rules requiring IaaS Providers to "ensure that foreign resellers of United States IaaS Products verify the identity of any foreign person that obtains an IaaS account (account) from the foreign reseller."[10] Commerce has taken additional steps to implement this portion of the AI EO in a new notice of proposed rulemaking (NPRM), discussed below.



9 *Id.; see also* definitions of IaaS Provider and IaaS Product, Exec. Order No. 13,984, 86 FR 6837 (Jan. 25, 2021), https://www.federalregister.gov/d/2021-01714.

10 "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," 88 FR 75191 (Oct. 30, 2023), https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence

II. NIST and DHS Standards

On April 29, 2024, NIST took a significant step toward implementing the AI EO by releasing four draft publications, including: *AI RMF Generative AI Profile* (NIST AI 600-1), *Secure Software Development Practices for Generative AI and Dual-Use Foundation Models* (NIST Special Publication (SP) 800-218A), *Reducing Risks Posed by Synthetic Content* (NIST AI 100-4), and *A Plan for Global Engagement on AI Standards* (NIST AI 100-5).[11]

Those four draft publications build upon existing documents from NIST, including the *NIST Artificial Intelligence Risk Management Framework* (AI RMF).[12] The AI RMF, released in January of 2023, was NIST's first comprehensive standards document regarding AI and deals with a wide range of AI-related topics including safety, transparency, privacy, and bias, among many others. The goal of the AI RMF is to "offer a resource to the organizations designing, developing, deploying, or using AI systems to help manage the many risks of AI and promote trustworthy and responsible development and use of AI systems."[13] As with most NIST documents, the AI RMF is "intended to be voluntary, rights-preserving, non-sector-specific, and use-case agnostic, providing flexibility to organizations of all sizes and in all sectors and throughout society to implement the approaches in the Framework."[14]

The AI RMF Generative AI Profile (AI Profile) is intended to help organizations in understanding risks posed by generative AI and identifying various actions for generative AI risk management. The document is intended to be a companion to AI RMF. The AI Profile contains 13 categories of risks and over 400 potential actions to manage those risks. Many of the risks are unrelated to national security, but many—such as those involving chemical, biological, radiological, and nuclear weapons; dangerous or violent recommendations; and information integrity—have a clear national security nexus.

Secure Software Development Practices for Generative AI and Dual-Use Foundation Models also builds upon prior NIST guidance and is focused on risks related to malicious training data adversely affecting generative AI systems. The publication provides guidance on dealing with training data and collecting training data, including actions such as analyzing training data for signs of "poisoning, bias, homogeneity and tampering."

Reducing Risks Posed by Synthetic Content is focused on the rise of synthetic content, including deepfakes, and lays out methods for detecting, authenticating, and labeling synthetic content, including measures such as watermarking and metadata recording. The report defines synthetic content as "information, such as images, videos, audio clips, and text, that has been significantly altered or generated by algorithms, including by AI."[15] Synthetic content can present a variety of risks, including national security risks relating to fake video or audio of political leaders.

Finally, *A Plan for Global Engagement on AI Standards* outlines NIST's plans to drive worldwide development of standards, cooperation and coordination, and information sharing. It seeks to outline both areas that are ripe for global standardization now, as well as areas that require additional research to identify appropriate standards.

In addition to NIST, on April 29, 2024, in accordance with the AI EO, the Department of Homeland Security (DHS) published *Safety and Security Guidelines for Critical Infrastructure Owners and Operators* (Safety Guidelines)[16] and portions of a report to the president on trends in AI related to chemical, biological, radiological, and nuclear (CBRN) weapons.[17] The Safety Guidelines highlight various AI risks for critical infrastructure and provide guidance to industry on mitigating those risks through best practices. The report also includes appendices that provide additional detail on certain cross-sector risks including attacks using AI, attacks on AI, and AI design and implementation failures. The Safety Guidelines are intended to correspond with and be used in conjunction with the AI RMF and other public guidance documents. While the CBRN report was not released in full, DHS released selected findings from the report as a part of a larger fact sheet on its efforts to reduce AI risks related to CBRN. The report highlights several AI risks related to CBRN production and proliferation, as well as the potential benefits of AI to counter CBRN threats.

11 *Department of Commerce Announces New Actions to Implement President Biden's Executive Order on AI, Department of Commerce* (April 29, 2024), https://www.commerce.gov/news/press-releases/2024/04/department-commerce-announces-new-actions-implement-president-bidens.

12 *Artificial Intelligence Risk Management Framework,* National Institute of Standards and Technology (Jan. 26, 2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

13 *Id.* at 2.

14 *Id.*

15 *Reducing Risks Posed by Synthetic Content,* National Institute of Standards and Technology (Apr. 2024), https://airc.nist.gov/docs/NIST.AI.100-4.SyntheticContent ipd.pdf.

16 *Safety and Security Guidelines for Critical Infrastructure Owners and Operators,* Department of Homeland Security (Apr. 29, 2024), https://www.dhs.gov/sites/default/files/2024-04/24_0426_dhs_ai-ci-safety-security-guidelines-508c.pdf.

17 *FACT SHEET: DHS Advances Efforts to Reduce the Risks at the Intersection of Artificial Intelligence and Chemical, Biological, Radiological, and Nuclear (CBRN) Threats,* Department of Homeland Security (Apr. 29, 2024), https://www.dhs.gov/sites/default/files/2024-04/24_0429_cwmd-dhs-fact-sheet-ai-cbrn.pdf.

These standards are not laws and, in many cases, are not linked to existing laws. Rather, the standards broadly aim to identify technical standards and best practices that industry can voluntary implement to mitigate potential risks arising from AI. While these standards are voluntary, they may nonetheless form the basis for later legal requirements. For example, it is possible that Congress or agency regulators will seek to require creators of generative AI models to implement watermarking to help identify synthetic content, as currently recommended by NIST.

While the standards are not scoped to promote compliance with any particular legal regime, adherence to the standards may nonetheless promote compliance. For instance, a company that implements NIST and DHS standards with respect to CBRN may be less likely to inadvertently violate export controls laws, which (as discussed below) tightly control certain information related to such weapons. In addition, given the absence of clear regulatory guidance from most agencies, adherence to the NIST and DHS standards may help companies demonstrate to regulators that their compliance programs are appropriately scoped to the risks posed by their use of AI and that they have carefully considered and sought to mitigate such risks. The existence of a robust, appropriately-scoped, and well-implemented compliance program is an explicit factor in enforcement decisions under certain regulatory regimes impacting AI, as outlined below.

III. Customer Identification Requirements for Certain AI Training and IaaS Providers

On January 29, 2024, the Department of Commerce issued a proposed rule to implement portions of the AI EO (and a prior EO targeting IaaS providers).[18] The proposed rule requires certain providers of IaaS products to implement customer identification programs (CIPs) to verify the identity of foreign customers.

A. CIP requirements

The CIP must first be able to determine whether an IaaS Account is being opened for a foreign or US person, by assessing whether both the customer itself (including both individual and entity customers) and "all beneficial owners" are US persons. If an IaaS provider is unable to determine that a potential customer and all beneficial owners are US persons, then the provider must apply the CIP in full to that customer or beneficial owner. The NPRM outlines several pieces of information that must be obtained, including full legal name or entity name, address, "means and source of payment for the Account," email, phone number, and internet protocol (IP) address used for account access or administration and the date and time of such access. In addition to collecting the above information, IaaS providers will also be required to verify the identity of a potential foreign customer and beneficial owners by use of documentary or non-documentary methods, outlined in further detail in the NPRM.

An IaaS provider would be obligated to notify Commerce about its CIP, and the CIP of each of its foreign resellers, through the submission of a "CIP certification form." The certification form calls for a variety of information such as the tools and procedures used for customer verification; the "mechanisms, services, software, systems, or tools used by the IaaS provider to detect malicious cyber activity;" procedures for supervising foreign resellers, and procedures for identifying when a foreign person transacts to train a large AI model with potential capabilities that *could be used* in malicious cyber-enabled activity, among other requirements. The certification also calls for a range of information regarding the IaaS provider, including its service offerings and customer base, number of employees, number of customers, and a list of all foreign resellers, among several other data points. The certification must also include an attestation that the CIP meets the enumerated regulatory requirements. An updated certification must then be submitted on an annual basis.

Notably, the requirement to maintain procedures to detect malicious cyber activity would mean the program is not just limited to understanding and verifying customer identification, but also requires ongoing monitoring of the substantive activities of a customer, something that may not fit neatly within the concept of a CIP program under other regimes.

The term "malicious cyber-enabled activities" is defined broadly to mean activities "that seek to compromise or impair the confidentiality, integrity, or availability of computer, information, or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon."[19]

The NPRM also provides examples of AI-related malicious cyber-enabled activities, including "social engineering attacks, vulnerability discovery, denial-of-service attacks, data poisoning, target selection and prioritization, disinformation or misinformation generation and/or propagation, and remote command-and-control of cyber operations."[20]

IaaS providers that "contract with, enable, or otherwise allow foreign resellers to resell their US IaaS products" would be obligated to ensure that such foreign resellers implement and maintain a CIP meeting the requirements of the rule.

Commerce may, at its discretion, conduct reviews of an IaaS provider's CIP "based on the Department's own evaluation of risks associated with a given CIP, US IaaS provider, or any of its foreign resellers."[21]

18 *Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities,* 89 FR 5698 (proposed Jan. 29, 2024) (to be codified at 15 C.F.R. 7). Comment period closed April 29, 2024; awaiting final rule, https://www.federalregister.gov/documents/2024/01/29/2024-01580/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious?ref=thestack.technology.

19 *Id.* at 5727.

20 *Id.*

21 *Id.* at 5730.

B. Exemption for providers with approved ADP

Under the NPRM, Commerce may exempt an IaaS provider from the CIP requirements upon a determination the "IaaS provider has established an Abuse of IaaS Products Deterrence Program (ADP)" meeting certain enumerated standards. Commerce may also make such a finding with respect to a foreign reseller, exempting the IaaS provider from the CIP rules with regard to that specific reseller. An ADP must be "designed to detect, prevent, and mitigate malicious cyber-enabled activities in connection with their Accounts and the IaaS Accounts of its foreign resellers" and must be appropriate given the size and complexity of the IaaS provider's business and products.

Among other requirements, an ADP must identify potential red flags for the accounts that the IaaS provider offers or maintains, contain measures to detect the existence of such red flags, and contain procedures to respond to any detected red flag to "prevent and mitigate malicious cyber-enabled activities." The ADP must be updated regularly and must contain requirements for a number of related matters such as employee training and oversight of foreign resellers. The NPRM contains significant additional detail on the requirements for ADPs.

C. Special measures for certain foreign jurisdictions and foreign persons

The NPRM would authorize Commerce to prohibit or impose conditions on (1) customers, potential customers, or accounts within certain foreign jurisdictions and (2) certain foreign persons upon a finding that "reasonable grounds exist for concluding that a foreign jurisdiction or foreign person is conducting malicious cyber-enabled activities using US IaaS products…." The NPRM contains additional detail on the process and criteria used for undertaking such evaluations. Any special measures are valid for 365 calendar days, but may be extended by Commerce. IaaS providers will have 180 days to comply with any special measures issued by Commerce.

D. Reporting of large AI model training

In addition to the CIP requirements, the NPRM would require IaaS providers to submit a report to Commerce when they have "knowledge" of a "covered transaction." The term "covered transaction" means a "transaction by, for, or on behalf of a foreign person which results or could result in the training of a large AI model with potential capabilities that could be used in malicious cyber-enabled activity."[22] It also includes developments or updates to a prior transaction that cause it have such a result or potential result.

The term "large AI model with potential capabilities that could be used in malicious cyber-enabled activity" means "any AI model with the technical conditions of a dual-use foundation model or otherwise has technical parameters of concern, that has capabilities that could be used to aid or automate aspects of malicious cyber-enabled activity…"[23] This includes, among other conduct, "social engineering attacks, vulnerability discovery, denial-of-service attacks, data poisoning, target selection and prioritization, disinformation or misinformation generation and/or propagation, and remote command-and-control of cyber operations."[24]

The term "dual-use foundation model" means:

An AI model that is trained on broad data; generally uses self-supervision; contains at least tens of billions of parameters; is applicable across a wide range of contexts; and that exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety, or any combination of those matters, such as by: (i) Substantially lowering the barrier of entry for non-experts to design, synthesize, acquire, or use chemical, biological, radiological, or nuclear (CBRN) weapons; (ii) Enabling powerful offensive cyber operations through automated vulnerability discovery and exploitation against a wide range of potential targets of cyber attacks; or (iii) Permitting the evasion of human control or oversight through means of deception or obfuscation.[25]

Importantly, as indicated above, models meet that definition "even if they are provided to end users with technical safeguards that attempt to prevent users from taking advantage of the relevant unsafe capabilities."[26]

Notably, the examples provided in (i)-(iii) above are merely illustrative and not exhaustive. The fact that technical safeguards cannot be considered when determining whether a model falls within the definition will serve to broaden, significantly, the range of models contained in that definition. The NPRM would not require any knowledge that an actor actually intends to use a dual-use foundation model for malicious purposes, only that the model "could" be used for malicious purposes. Consequently, many IaaS providers will likely focus on the size of the AI model, rather than the potential use cases, when considering their reporting obligations.[27] Commerce may publish additional definitional detail in subsequent "interpretive rules." IaaS providers would also be required to obligate their foreign resellers to submit a report when they have "knowledge" of a "covered transaction."

22 *Id.* at 5733.

23 *Id.* at 5702.

24 *Id. at 5727.*

25 *Id.* at 5726.

26 *Id.*

27 *See, e.g., Disrupting malicious uses of AI by state-affiliated threat actors,* OpenAI (Feb. 14, 2024), https://openai.com/blog/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors.

IV. AI Export Controls

US export controls are intended to prevent potentially sensitive "items" from being used by US adversaries for malign purposes. The Export Administration Regulations (EAR) control the export, reexport, and transfer (in country) of dual-use items and certain less sensitive military items.[28] The International Traffic in Arms Regulations (ITAR) apply to defense articles and defense services.[29] This white paper will principally focus on the EAR, but will touch briefly on the ITAR, as well.

The EAR can apply to AI in a number of complex and sometimes unexpected ways. These include potential controls on an AI model or system itself, as well as the potential for an AI model to generate export-controlled content or to have export-controlled content in its training data.

A. Export controls basics

Items subject to the EAR include not only physical items (e.g., advanced semiconductors used for AI) but also intangible items, including software and technology. Technology, which is broadly defined under the EAR, can take the form of narrative descriptions, schematics, blueprints, and more.[30] Items "subject to the EAR" are subject to US jurisdiction regardless of where the item is located around the world. Thus, jurisdiction attaches to the item itself even if it moves across borders. It is also important to note that the concept of an export includes not only the physical shipment or digital transmission of an item outside of the United States (or, in the case of a reexport, from one foreign country to another), but also so-called "deemed exports" or "deemed reexports," which arise when technology is released to a non-US person. For example, a deemed export can occur if a non-US person visits a US facility and views technology related to items under development at the facility.[31]

Items subject to the EAR may require a license for the export, reexport, or transfer of the item. Whether a license is required can be a complex analysis that depends on the item in question, the jurisdictions in question, and end-use or end-user of the item. Items subject to heightened US licensing requirements under the EAR are included on the Commerce Control List (CCL) pursuant to an alphanumeric code known as an export controls classification number (ECCN). Inclusion on the CCL does not mean a license is required for all exports, reexports, or transfers of the item, but means the item is subject to at least some heightened licensing requirements that are not applicable to items subject to the lowest levels of control, known as "EAR99."

Items can be "subject to the EAR" for a number of reasons, including because they are located in the United States; are "US origin;" or, in certain circumstances, are foreign-made items that incorporate or are bundled or comingled with US-origin items. Under the "Foreign Direct Product Rules," certain foreign-produced items that are "direct products" of specified technology or software or of a plant or major component of a plant that is itself the "direct product" of specified technology and software may also be "subject to the EAR."

The EAR also provides a number of categories of items that are not "subject to the EAR." For example, data "published" on internet sites available to the public are not considered controlled technology or software subject to the EAR.

With respect to AI, the EAR can apply to AI software systems and physical infrastructure (e.g., advanced semiconductors and semiconductor manufacturing equipment) used to train or operate AI systems. It can also apply to material included in training data and to content that is generated by AI systems (e.g., a large multimodal model that provides a technical description or produces a detailed image or blue print).

30 15 C.F.R. § 772.1.

31 A non-US person or "foreign person" includes: "Any natural person who is not a lawful permanent resident of the United States, citizen of the United States, or any other protected individual as defined by 8 U.S.C. 1324b(a)(3). It also means any corporation, business association, partnership, trust, society or any other entity or group that is not incorporated in the United States or organized to do business in the United States, as well as international organizations, foreign governments and any agency or subdivision of a foreign government (e.g., diplomatic mission)." 15 C.F.R. § 772.1. While outside the scope of this white paper, employers should be aware that restricting positions with access to export-controlled items solely on the basis of national origin or citizenship status can violate anti-discrimination laws.

B. AI software

While there is no ECCN that broadly controls general purpose AI software, there are dozens of ECCNs that could potentially control a given piece of application-specific AI software.[32] Some of these ECCNs specifically describe AI software while most are broader ECCNs, often called "catchall" ECCNs, that apply broadly to certain types of software. A full description of the potentially applicable ECCNs is beyond the scope of this white paper, but below we offer a few illustrative examples.

ECCN 3D001 – Certain software for use in the development or production of specified electronic components

- ECCN 3A090 controls a variety of specified integrated circuits. ECCN 3D001 controls, among other things, "'Software' 'specially designed' for the 'development' or 'production' of commodities controlled by 3A090 …." Therefore, certain AI systems that are intended to optimize electronic circuit design, for example, could be controlled under 3D001.

ECCN 6D991 – Certain software for use with advanced cameras

- ECCN 6A003 controls certain "cameras, systems or equipment, and 'components' therefor" meeting enumerated criteria. 6D991 controls certain software "'specially designed' for the 'development', 'production', or 'use' of commodities controlled by" 6A003 and other ECCNs. Therefore, an AI system intended to support the use of a camera controlled by 6A003 could be controlled under 6D991.

ECCN 8D001 – Certain Software for Unmanned Submersible Vehicles

- ECCN 8A001 controls certain unmanned submersible vehicles. ECCN 8D001 controls software "'specially designed' or modified for the 'development,' 'production' or 'use' of equipment or materials, controlled by 8A …." Therefore, AI systems that control the operation of an unmanned submersible vehicle could be controlled under ECCN 8D001.

As noted above, there are myriad other examples of ECCNs that might potentially apply to a given piece of AI software.

C. Controls on AI model training data and outputs

Regardless of whether the AI software itself is controlled, it is important to consider whether any of the model's training data or outputs might be controlled.

With respect to training data, AI systems are trained on massive quantities of data, and, depending on the source of the data in question, certain of the data could be export controlled. Knowing whether any of the model training data are export controlled is important for a number of reasons.

First, having controlled training data makes it more likely that a system will produce controlled outputs. For example, a model asked about manufacturing drones is more likely to provide responses containing EAR-controlled technology, if the model is trained on such data (although, as discussed below, it may be possible for a model trained on no EAR-controlled technology to generate a response containing such technology). Researchers have also demonstrated that many models are vulnerable to so-called "divergence attacks," in which models are provoked to directly emit training data.[33]

Second, having controlled training data could lead to a violation if the data is exported, reexported, or transferred or a "deemed export" or "deemed reexport" occurs. In the case of supervised learning, it is often necessary for a human or another machine to label the data so that the AI system can learn from the labeled data. Human labeling is often done by employees outside the United States, meaning data is often exported from the home country of the AI software company to the country where the human labelers reside. Many AI software companies also pool talent from leading AI scientists around the world, meaning a company may have employees, contractors, or partners in a number of jurisdictions, all of whom have access to the training data.

Third, having controlled training data makes it more likely an AI model will generate content that is "subject to the EAR."[34] For example, in certain cases, foreign made technology can be subject to the EAR when it is comingled with US-origin technology. This is known as the "*de minimis rule*" and typically requires a calculation of the value of the US-origin technology as compared to the total value of the foreign technology. Therefore, an AI system that is operated outside the United States and produces an output that is based largely on non-US data may still produce technology that is subject to the EAR if the training data used to generate the output contains US-origin content exceeding the relevant *de minimis* threshold. However, trying to conduct a de minimis rule analysis on an AI model may be extremely challenging. It may not be clear how the AI system arrived at the output and, therefore, could be unclear which specific pieces of data produced the output. Trying to value the data used and the outputs could also be quite challenging.

Even if none of the training data are controlled, it may be possible, theoretically, for the output of the AI system to be controlled technology or software. This is a particularly complex issue for generative AI, including language models (LLMs). For example, regardless of the nature of the training data, an AI system that generated technology for certain optical sensors (ECCN 6E992) or technology for facilities designed to produce certain chemicals (ECCN 1E350) may, potentially, create controlled outputs. In such instances, the AI model may be combining a variety of information that is not considered "technology" (perhaps because it is a general systems description or other high-level overview) and, at least in theory, create something new that is sufficiently detailed to constitute "technology."

32 Recent reports suggest that the Commerce Department is exploring whether to restrict the export of certain proprietary AI models. Further, a bipartisan group of lawmakers has introduced legislation to impose export controls on AI models. *Reuters, US lawmakers unveil bill to make it easier to restrict exports of AI models* (May 9, 2024), https://www.reuters.com/technology/us-lawmakers-unveil-bill-make-it-easier-restrict-exports-ai-models-2024-05-10/. Although the ultimate outcome of those efforts remains uncertain, they demonstrate an increasing interest and urgency among US policymakers in further restricting access to US-developed AI models outside of the United States.

33 *See, e.g.*, Milad Nasr et al., *Scalable Extraction of Training Data from (Production) Language Models,* arXiv:2311.17035 preprint (Nov. 28, 2023), https://arxiv.org/abs/2311.17035.

34 15 CFR § 734.7. In principle, this also applies to data controlled under other export controls regimes, such as the ITAR, discussed below.

With that said, one key and unanswered question in this area is whether a model that merely combines existing public data, as many of today's models do, can in fact generate something truly new such that it would go beyond what is publicly available (i.e., "published").[35] The answer to that question turns on a number of considerations including the nature of the training data (i.e., whether it is exclusively public data) and the capabilities of the model (i.e., is it capable of creating something new or just compiling existing data). It also raises questions of how BIS may interpret the reach of its own regulations and whether the agency might find that a new presentation or compilation of public data was sufficiently different from the existing public sources to constitute controlled technology, even if that technology was not going beyond what a human could, in theory, cobble together from public sources. At present, such an approach would seemingly go well beyond existing BIS guidance and be difficult to administer in practice. These questions may become more salient in the future, however, as frontier models evolve beyond making linguistic predictions toward being able to generate truly new ideas.

Additionally, there may also be questions as to whether the output is "subject to the EAR." For example, if a model uses non-US servers, has no controlled US-origin training data, and is operated entirely outside the United States it could be the case that the output is not "subject to the EAR." Although these appear to be important issues for many users of generative AI models, there is currently no clear guidance from BIS as to when a model's output might be considered US-origin or otherwise subject to the EAR.

Because it is often not possible to predict, or even fully understand, how an AI system will arrive at a given conclusion or generate a given piece of content, trying to implement safeguards to prevent the system from generating export-controlled content can be particularly challenging. In other cases, the intent of the AI model may be to create controlled content (e.g., for AI models intended for specific industries, rather than general use). In such scenarios, it is important to understand whether the individuals using the system are US persons as opposed to non-US nationals (as well as the nationality and visa/immigration status of the latter). The ultimate end-use and end-user of the outputs are also likely to be relevant considerations.

There are a number of steps that creators of generative AI systems can take to try to minimize the possibility an AI model will produce export-controlled technology. Such measures include training data curation, model design and training, concept erasure,[36] post-training policies and filters, periodic updates and monitoring, and user prompt monitoring.

D. AI hardware

The area of US export controls with the most significant focus in recent years has been, unquestionably, advanced semiconductors (also called integrated circuits or "ICs") and semiconductor manufacturing equipment (SME).

While advanced semiconductors present an array of national security and foreign policy considerations, BIS has made clear that use of advanced chips to train cutting edge AI models is a major driver of recent regulatory changes. For example, in announcing recent updates to rules regarding ICs and SME, BIS explained the changes are intended to counter China's ability to train frontier AI models that have the most significant potential for advanced warfare applications, including unmanned intelligent combat systems, enhanced battlefield situational awareness and decision making, multidomain operations, automatic target recognition, autopiloting, missile fusion, precise guidance for hypersonic platforms, and cyber attacks.

The EAR rules related to ICs and SME are among the most complex areas of the EAR, requiring a deep understanding of both the regulations and the underlying technology. While a complete exploration of those rules is beyond the scope of this white paper, we provide a high-level summary of the rules with a particular focus on recent enhancements to BIS rules announced in 2022[37] and 2023[38]. Among other provisions, those regulatory enhancements:

- Add certain advanced and high-performance computing chips and computer commodities that contain such chips to the CCL.
  - With respect to ICs, these ECCNs rely on a number of control parameters including the IC's total performance, performance density, and the intended use of the IC, including whether it is "designed or marketed" for use in a datacenter (with non-datacenter chips generally subject to less stringent controls).
- Impose and expand licensing requirements on the export of advanced chips, with a presumption of denial, to certain sensitive jurisdictions.
- Impose controls on additional types of SME by adding such items to the CCL and imposing license requirements for certain sensitive jurisdictions.
- Establish a worldwide licensing requirement for the export of controlled chips to any company that is headquartered in certain sensitive jurisdictions or whose ultimate parent company is headquartered in those jurisdictions.
- Impose new end use and end user-based restrictions prohibiting the export of certain items when there is knowledge the item is intended for certain destinations, end uses, or end users related to supercomputers, advanced-node ICs, and SME.
- Create a notification requirement for the export of certain high-end gaming chips used to train AI models.
- Expand the scope of the EAR over certain foreign-produced advanced computing items and foreign produced items for supercomputer end uses.

35 As a general matter, and with limited exceptions, unclassified technology or software that is published, and made available to the public without restriction, is not subject to the EAR. 15 C.F.R. § 734.7.

36 For a discussion of concept erasure, see Nupur Kumari et al., *Ablating Concepts in Text-to-Image Diffusion Models,* arXiv preprint (Aug. 16, 2023), https://arxiv.org/abs/2303.13516.

37 *Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification*, 87 FR 62215 (Oct. 13, 2022), https://www.federalregister.gov/d/2022-21658.

38 *Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections,* 88 FR 73517 (Oct. 25, 2023), https://www.federalregister.gov/d/2023-23055; "Export Controls on Semiconductor Manufacturing Items," 88 FR 73424 (Oct. 25, 2023), https://www.federalregister.gov/d/2023-23049.

- Expand the scope of foreign-produced items subject to license requirements to certain entities on the Entity List.
- Restrict the ability of US persons to engage in certain activities in support of advanced semiconductor manufacturing involving specified destinations even when no item subject to the EAR is involved.

BIS also imposed a series of stringent export controls targeting Russia and has created a "Common High Priority Items List" to identify items that "pose a heightened risk of being diverted illegally to Russia because of their importance to Russia's war efforts."[39] Among other items, the list includes various types of ICs and IC components.

New users of the CCL may also notice controls on "neural network integrated circuits" at ECCN 3A001.a.9 and "neural computers" at ECCN 4A004.b. However, because most current AI models operate on standard computers and use ICs such as graphical processing units (GPUs) these controls are not typically implicated by today's AI systems. As research continues to advance, it is possible these controls will become more relevant in the future.

E. Data

In addition to semiconductors, data is the other critical building block of AI. As explained above, data may be controlled if it constitutes "technology" under the EAR (or is controlled by another export controls regime). Much of the data used to train AI models may not be controlled either because it does not constitute "technology" or is not subject to the EAR (e.g., data that is "published" on the internet). As US adversaries continue to train advanced AI models, and rely on data to do so, US policymakers may seek additional limitations on the sharing of such data. As described below in the discussion on sensitive personal data, this process has already begun, and may continue to expand over time either via export controls or other independent regimes.

F. Entity list

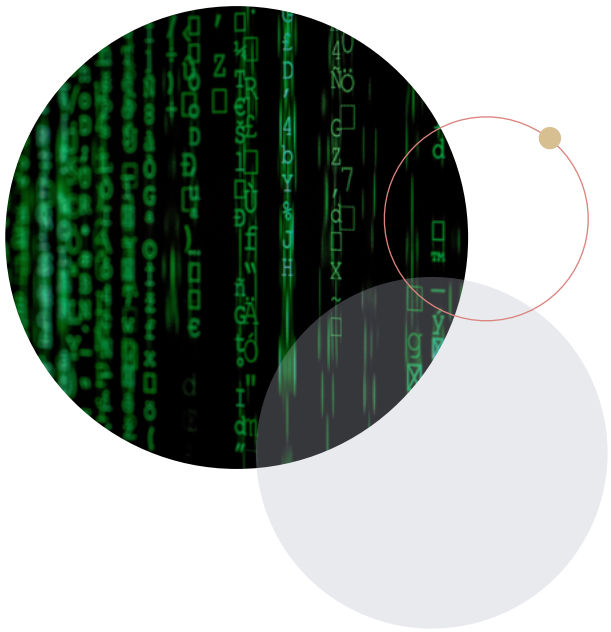
The EAR also contain targeted restrictions focused on specific entities included on the Entity List. The Entity List subjects specified businesses, research institutions, governments, and other persons to enhanced licensing requirements for the export, reexport, or transfer of certain items. Those requirements vary, with some entities subject to a licensing requirement with respect to all items subject to the EAR and others, by contrast, face licensing requirements for a more limited set of items. Entities on the Entity List can also face heightened restrictions with respect to the foreign direct product rule, discussed above, and are not able, generally, to take advantage of license exceptions contained in the EAR.

The Entity List has been used to target a number of actors in the AI industry and adjacent sectors, including companies involved in advanced IC manufacturing for AI applications.[40] Members of Congress have also called on the administration to add other AI companies to the list and to use the Entity List more aggressively going forward.[41]

The Entity List tends to be most effective when the targeted entity uses items subject to the EAR as part of its business, making it a somewhat narrower tool than other trade restrictions, such as OFAC sanctions, discussed below. Nevertheless, it has become an increasingly utilized tool in recent years and is likely to be a key component of US national security controls targeting AI in the future.

G. ITAR

While this white paper is principally focused on dual-use export controls contained in the EAR, it is worth noting that AI with military applications may be controlled under the ITAR. The ITAR controls defense articles, defense services, and related technical data, the latter of which includes software that is directly related to defense articles. Generally speaking, a license or other authorization is required for the export, reexport, or transfer of ITAR-controlled items. In addition, persons in the United States engaged in the business of manufacturing, exporting, or temporarily importing defense articles, or furnishing defense services, are required to register with the Department of State's Directorate of Defense Trade Controls (DDTC), which administers the ITAR. Items controlled under the ITAR are enumerated in the United States Munitions List (USML).



39 *Common High Priority Items List, Bureau of Industry and Security,* (Feb. 23, 2024), https://www.bis.doc.gov/index.php/all-articles/13-policy-guidance/country-guidance/2172-russia-export-controls-list-of-common-high-priority-items.

40 *Commerce Adds 36 to Entity List for Supporting the People's Republic of China's Military Modernization, Violations of Human Rights, and Risk of Diversion,* Bureau of Industry and Security (Dec. 15, 2022), https://www.bis.gov/press-release/commerce-adds-36-entity-list-supporting-peoples-republic-chinas-military.

41 Edward Wong, Mark Mazzetti and Paul Mozur, *Lawmakers Push U.S. to Consider Trade Limits With A.I. Giant Tied to China,* New York Times (Jan. 9, 2024), https://www.nytimes.com/2024/01/09/us/politics/ai-china-uae-g42.html.

V. ICTS Rule

In January 2021, the Department of Commerce published an interim final rule creating a new process for the executive branch to review transactions involving information and communications technology and services (ICTS) and to determine whether those transactions present national security risks.[42]

After some delay, on June 16, 2023, Commerce published a final rule, which largely retained the substance of the interim rule with a few minor modifications to clarify the definitions and criteria relevant to evaluating whether certain information and communications technology supply chain transactions present an undue or unacceptable risk to US national security.[43] When a qualifying ICTS transaction involves "foreign adversaries" and presents certain "undue or unacceptable risks" to the United States, the rule (ICTS Rule) allows Commerce to either block the transaction or impose risk-mitigation measures.

The ICTS Rule implements Executive Order 13873, *Securing the Information and Communications Technology and Services Supply Chain,*[44] which prohibits transactions involving certain foreign ICTS that present (1) an undue risk of sabotage or subversion to ICTS in the United States, (2) an undue risk of catastrophic effects on the security or resiliency of critical infrastructure or the digital economy in the United States, or (3) an unacceptable risk to US national security or the security and safety of US persons.

The ICTS Rule also implements EO 14034, *Protecting Americans' Sensitive Data from Foreign Adversaries.* President Biden issued Executive Order 14034 in June 2021,[45] which directed the Secretary of Commerce to evaluate the risks posed by connected software applications, commonly called "apps." The order identified additional criteria for Commerce to consider when evaluating transactions involving apps.

A. Scope of the ICTS rule

The ICTS Rule contains several criteria for a transaction to be covered by the ICTS Rule's review process.

First, the ICTS Rule's review process regulates ICTS transactions. "ICTS transactions" is broadly defined as:

> any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service, including ongoing activities, such as managed services, data transmission, software updates, repairs, or the platforming or data hosting of applications for consumer download. An ICTS Transaction includes any other transaction, the structure of which is designed or intended to evade or circumvent the application of the Executive Order.[46]

Under this sweeping definition, the ICTS Rule could subject a wide range of commercial interactions to scrutiny. It is important to note that the definition gives Commerce the authority not only to review individual ICTS transactions, but also entire classes of ICTS transactions.

"ICTS" is defined under the Rule as any:

> hardware, software, including connected software applications, or other product or service, including cloud-computing services, primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means (including electromagnetic, magnetic, and photonic), including through transmission, storage, or display.[47]

Thus, the term covers a broad array of technologies and services, including artificial intelligence, as well as internet systems, wireless networks, cellular phones, computers, satellite systems, quantum computing, and cloud computing services. The ICTS Rule also includes a broad category of "connected software applications" – i.e., "apps" – as ICTS.

Second, the ICTS transaction in question must be "property in which any foreign country or a national thereof has an interest (including through an interest in a contract for the provision of a technology or service)."[48]

Third, a transaction must involve ICTS designed, developed, manufactured, or supplied by persons or entities owned by, controlled by, or subject to the jurisdiction of a "foreign adversary."[49] The ICTS Rule sets out various criteria for determining whether this requirement is met, including the location of the transaction parties' facilities, ties between transaction party officials and a foreign adversary, and the laws in the jurisdiction in which a transaction party operates.[50] Foreign adversaries currently include China (including Hong Kong), Russia, Cuba, Iran, North Korea, and Venezuela.

42 *See* 15 C.F.R. Part 7. *See also Securing the Information and Communications Technology and Services Supply Chain,* 86 FR 4923 (Jan. 19, 2021), https://www.federalregister.gov/documents/2021/01/19/2021-01234/securing-the-information-and-communications-technology-and-services-supply-chain.

43 *See Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications,* 88 FR 39353 (Jun. 16, 2023), https://www.federalregister.gov/d/2023-12925.

44 Exec. Order 13873, 88 FR 22689 (May 15, 2019), https://www.federalregister.gov/d/2019-10538.

45 Exec. Order 14034, 86 FR 31423 (Jun. 9, 2021), https://www.federalregister.gov/d/2021-12506.

46 15 C.F.R. Part 7.2.

47 Id.

48 *See* 15 C.F.R. § 7.3(a)(2).

49 15 C.F.R. § 7.100(c).

50 *Id*. at (c)(1)-(4)

Finally, an ICTS transaction must satisfy several other jurisdictional criteria to be subject to the ICTS Rule's review process. Most critically, the transaction must involve one of the categories of technology enumerated by the Rule. The listed technology categories include, among other things, so-called "emerging technology." "Emerging technology" in this context is defined as "ICTS integral to *artificial intelligence and machine learning*, quantum key distribution, quantum computing, drones, autonomous systems, or advanced robotics."[51] Thus, the ICTS Rule explicitly regulates ICTS transactions involving AI technology. It is also possible that transactions involving AI could be captured under one of the other enumerated categories of technology set out by the ICTS Rule, such as AI used in sectors designated as critical infrastructure pursuant to the National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22), which covers a broad array of sectors, including, among others, the communications and information technology sectors.[52] The ICTS Rule could apply, then, to a very wide range of transactions involving AI with sufficient ties to a "foreign adversary."

B. Outlook for ICTS enforcement

The ICTS Rule is a relatively new addition to the US government's regulatory toolkit, and it has been used sparingly to date. However, the Commerce Department has issued subpoenas to multiple Chinese companies that provide ICTS in the United States and has begun a rulemaking process targeting so-called "connected vehicles," discussed below.[53] Although the manner in which the Commerce Department may ultimately utilize the ICTS Rule is still uncertain, its applicability to AI is unquestioned and its potential impact could be substantial, as it provides Commerce with broad and highly discretionary authority to prohibit or impose conditions on transactions involving AI with sufficient ties to a "foreign adversary."

Commerce recently appointed the first Executive Director of the Office of Information and Communications Technology and Services (OICTS), which is charged with implementing the rule.[54] It seems likely that as Commerce continues to develop its team, expertise, and regulatory and enforcement infrastructure, it will move to employ the ICTS Rule more frequently and aggressively, including as a means to regulate the use and availability of certain AI products and services.

C. ANPRM for connected vehicles

On February 29, 2024, Commerce announced a first of its kind action by initiating a rulemaking to prohibit or impose conditions on certain transactions involving foreign technology used in so-called "connected vehicles" or "CVs."[55] The advance notice of proposed rulemaking (ANPRM), explains that "BIS is considering proposing rules that would prohibit certain ICTS transactions or classes of ICTS transactions by or with persons who design, develop, manufacture, or supply ICTS integral to CVs" and are persons owned by, controlled by, or subject to the jurisdiction or direction of a "foreign adversary."[56] BIS is also considering allowing market participants to engage in otherwise prohibited transactions if they can demonstrate that any national security risks can be "sufficiently mitigated using measures that are monitorable."[57]

BIS is considering defining CV to mean "an automotive vehicle that integrates onboard networked hardware with automotive software systems to communicate via dedicated short-range communication, cellular telecommunications connectivity, satellite communication, or other wireless spectrum connectivity with any other network or device."[58] It adds, "Such a definition would likely include automotive vehicles, whether personal or commercial, capable of global navigation satellite system (GNSS) communication for geolocation; communication with intelligent transportation systems; remote access or control; wireless software or firmware updates; or on-device roadside assistance."[59] That definition is quite broad and would seemingly include nearly all recently manufactured vehicles.

The ANPRM explains that BIS is concerned with a wide-range of national security risks, including those posed by fully autonomous vehicles and vehicles with self-driving features or modes, many of which are powered by AI. Therefore, AI is clearly one of several key motivating risks behind the rulemaking process.

While the ANPRM is the first time BIS has sought to implement restrictions on a class of transactions under the ICTS rules it is unlikely to be the last. As OICTS continues to build out its capabilities and pursue its core policy objectives, it seems likely additional classes of transactions will be targeted in the future. AI and AI-powered products would seem to be among the most likely targets of such measures.

51 15 C.F.R. § 7.3(a)(4).

52 *National Security Memorandum on Critical Infrastructure Security and Resilience,* White House (Apr. 30, 2024), https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/. NSM-22 rescinded and replaced Presidential Policy Directive 21 of February 12, 2023.

53 *U.S. Department of Commerce Statement on Actions Taken Under ICTS Supply Chain Executive Order," Department of Commerce* (Apr. 13, 2021), https://www.commerce.gov/news/press-releases/2021/04/us-department-commerce-statement-actions-taken-under-icts-supply-chain; *See also* Mackenzie Hawkins, Josh Wingrove, and Jennifer Jacobs, *Biden administration may restrict imports of Chinese EVs and their parts no matter where they are built,* Fortune (Feb. 9, 2024), https://fortune.com/asia/2024/02/09/biden-administration-restrict-imports-chinese-evs-parts-built/.

54 *See BIS Announces Appointment of Elizabeth 'Liz' Cannon As Executive Director of Office of Information and Communications Technology and Services,* Bureau of Industry and Security (Jan. 22, 2024), https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3438-press-release-liz-cannon/file.

55 89 FR 15066 (Mar. 1, 2024), https://www.federalregister.gov/documents/2024/03/01/2024-04382/securing-the-information-and-communications-technology-and-services-supply-chain-connected-vehicles.

56 *Id.* at 15067.

57 *Id.*

58 *Id.* at 15068.

59 *Id.*

VI. Personal Data Controls

On February 28, 2024, the Biden administration announced the creation of a new national security regulatory regime that will prohibit or restrict certain transactions involving bulk sensitive US personal data or government-related data and specified "countries of concern."

The Biden administration announced the regime in a new executive order, *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern* (EO 14117), which was accompanied by an ANPRM issued by the National Security Division (NSD) of the Department of Justice (DOJ), the component and agency with primary responsibility for implementing and enforcing the forthcoming regulations.[60]

Shortly following the issuance of EO 14117, on April 24, 2024, President Biden signed into law a broad national security bill focused on providing funding to key allies and enhancing a number of US sanctions and export controls measures. Among the law's many provisions was the *Protecting Americans' Data from Foreign Adversaries Act of 2024* (PADFAA), which prohibits data brokers from making available personally identifiable sensitive data to certain foreign adversaries.[61]

PADFAA contains a number of key differences from EO 14117 and is both narrower and broader than the EO in certain respects. PADFAA also gives enforcement authority to the Federal Trade Commission (FTC), rather than DOJ. The result is that, at the time of this writing, it is unclear what will happen to EO 14117 and the DOJ rulemaking process. It is possible the rulemaking process continues as planned, is scrapped entirely, or is tailored to more closely align to PADFAA.

What is clear is that the rapid advancement of AI was a key motivating factor behind the EO and PADFAA. EO 14117 specifically highlights that national security risks related to US personal data have become more acute due to improvements in AI and its ability to analyze and manipulate data sets. Bulk sensitive personal data can also be used in the creation and refinement of AI models and other advanced technologies.

Given the uncertainty over these regimes at the time of this writing, the below section walks through both regimes and concludes by analyzing some of the key differences between the two.

A. EO 14117

i. Overview of regime

The new regime, if implemented, will broadly prohibit certain transactions and impose restrictions on other transactions involving "bulk sensitive personal data" or "government-related data" and "covered persons" associated with "countries of concern." The ANPRM uses the term "covered data transaction," which it defines as, "any transaction that involves any bulk US sensitive personal data or government-related data and that involves: (1) data brokerage; (2) a vendor agreement; (3) an employment agreement; or (4) an investment agreement."[62]

The ANPRM contemplates prohibiting certain "highly sensitive transactions" falling into two categories: (1) data brokerage transactions and (2) genomic data transactions involving the transfer of bulk human genomic data or biospecimens from which such data can be derived. It contemplates imposing restrictions on three categories of transactions, including: (1) vendor agreements involving the provision of goods and services (including cloud-service agreements); (2) employment agreements; and (3) investment agreements.

ii. Countries of concern and covered persons

The ANPRM states that countries of concern are likely to include China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, and Venezuela, which is consistent with the approach taken in other newly created national security regulatory regimes, including the new ICTS rules, discussed above.

The ANPRM indicates DOJ is likely to define "covered person" broadly to include:

1. An entity that is 50 percent or more owned, directly or indirectly, by a country of concern, or that is organized or chartered under the laws of, or has its principal place of business in, a country of concern;
2. An entity that is 50 percent or more owned, directly or indirectly, by an entity described in category (1) or a person described in categories (3), (4), or (5);
3. A foreign person who is an employee or contractor of a country of concern or of an entity described in categories (1), (2), or (5);
4. A foreign person who is primarily resident in the territorial jurisdiction of a country of concern; or
5. Any person designated by the Attorney General as being owned or controlled by or subject to the jurisdiction or direction of a country of concern, or as acting on behalf of or purporting to act on behalf of a country of concern or covered person, or knowingly causing or directing a violation of these regulations.[63]

60 *Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern* 89 FR 15780 (Apr. 19, 2024), https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and. Comment period closed April 19, 2024.

61 *Protecting Americans' Data from Foreign Adversaries Act of 2024,* Division I of Pub. L. No. 118-50, https://www.congress.gov/bill/118th-congress/house-bill/815/text#H3954D39129FA4D099436402B9DE6D8AB.

62 *Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern* 89 FR 15780 at 15788, Comment period closed April 19, 2024. (Apr. 19, 2024), https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and.

63 *Id.* at 15790.

iii. Prohibited covered data transactions

As noted above, DOJ is contemplating a prohibition on two categories of transactions involving covered persons.

First, the ANPRM contemplates a prohibition on US persons knowingly engaging in a covered data transaction involving "data brokerage" with any foreign person unless the US person contractually requires that the foreign person refrain from engaging in a subsequent covered data transaction involving the same data with a country of concern or covered person. DOJ notes this is the only portion of the rules that is likely to regulate conduct involving third countries.

The term "data brokerage" is defined in the ANPRM to mean "the sale of, licensing of access to, or similar commercial transactions involving the transfer of data from any person (the provider) to any other person (the recipient), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data."[64]

Second, the ANPRM contemplates a prohibition on US persons knowingly engaging in any covered data transaction with a country of concern or covered person that provides that country of concern or covered person with access to bulk US sensitive personal data that consists of human genomic data, or to human biospecimens from which such data could be derived.

DOJ is also contemplating a prohibition on US persons knowingly "directing" any covered data transaction by a foreign person that would be prohibited (including restricted transactions that do not comply with the security requirements) if engaged in by a US person.

iv. Restricted covered data transactions

The ANPRM contemplates a prohibition on covered data transactions involving: (1) vendor agreements; (2) employment agreements; and (3) investment agreements, each as defined in the ANPRM, unless such transactions comply with certain security requirements enumerated in the rules. The precise security requirements remain under consideration. The ANPRM states the security requirements are likely to fall within three broad categories, indicating a restricted covered data transaction would be permissible if a US person:

1. implements Basic Organizational Cybersecurity Posture requirements;
2. conducts the covered data transaction in compliance with the following four conditions: (a) data minimization and masking; (b) use of privacy preserving technologies; (c) development of information-technology systems to prevent unauthorized disclosure; and (d) implementation of logical and physical access controls; and
3. satisfies certain compliance-related conditions, such as retaining an independent auditor to perform annual testing and auditing of the requirements in (1) and (2) above, for so long as the US person relies on compliance with those conditions to conduct the restricted covered data transaction.[65]

The ANPRM contemplates a number of important exemptions, including with respect to certain financial transactions, transactions within multinational US companies, activities of the US government, and transactions required or authorized by federal law or international agreements. These exemptions may be critically important for some members of industry who would otherwise face significant operational challenges due to the new regulatory scheme.

DOJ is also contemplating a number of broad, categorical exclusions from the concept of "investment agreements" for investments that are "passive investments that do not convey the ownership interest or rights (including those that provide meaningful influence that could be used to obtain such access) that ordinarily pose an unacceptable risk to national security because they may give countries of concern or covered persons access to bulk sensitive personal data or government-related data."[66] For example, certain investments by limited partners in investment funds may fall within this exemption.

Because the new regime will be based on statutory authority contained in the International Emergency Economic Powers Act (IEEPA), DOJ states that the rules will also contain certain statutory exemptions including for personal communications and "information" and "informational materials," among other exemptions.

Of particular relevance for AI companies, the ANPRM contemplates an exclusion from the definition of sensitive personal data for "data that is lawfully available to the public from a Federal, State, or local government record or in widely distributed media (such as court records or other sources that are generally available to the public through unrestricted and open-access repositories)."[67] This is likely to be an important carveout for data sets that are scraped from public sources. However, it will be important for AI companies to understand when data sets are derived purely from public sources or when they are combined with other data that may not fall into that exemption.

64 *Id.* at 15788.

65 89 FR 15780, 15795 (Apr. 19, 2024).

66 *Id.* at 15789.

67 *Id.* at 15786.

v. Categories and quantity of bulk data

As discussed above, covered data includes both "sensitive personal data" and "government-related data." The ANPRM contemplates six categories of "sensitive personal data," including:

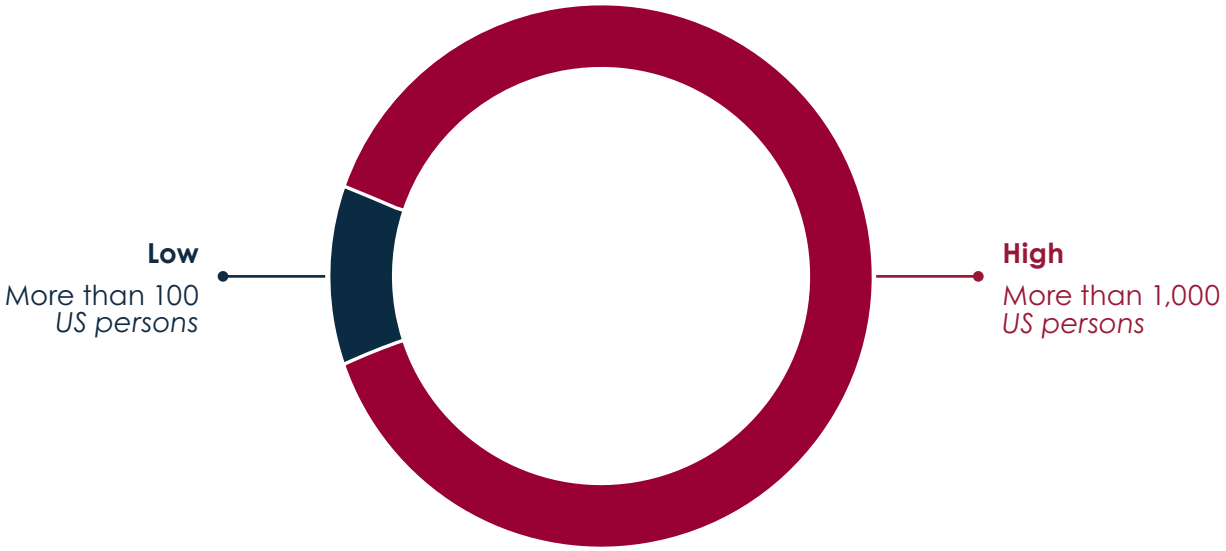
- certain enumerated covered personal identifiers;
- precise geolocation data;
- biometric identifiers;
- human genomic data;
- personal health data; and
- personal financial data.

Each of these categories is defined in considerable detail in the ANPRM and will likely be further refined in the proposed rule and final rule.

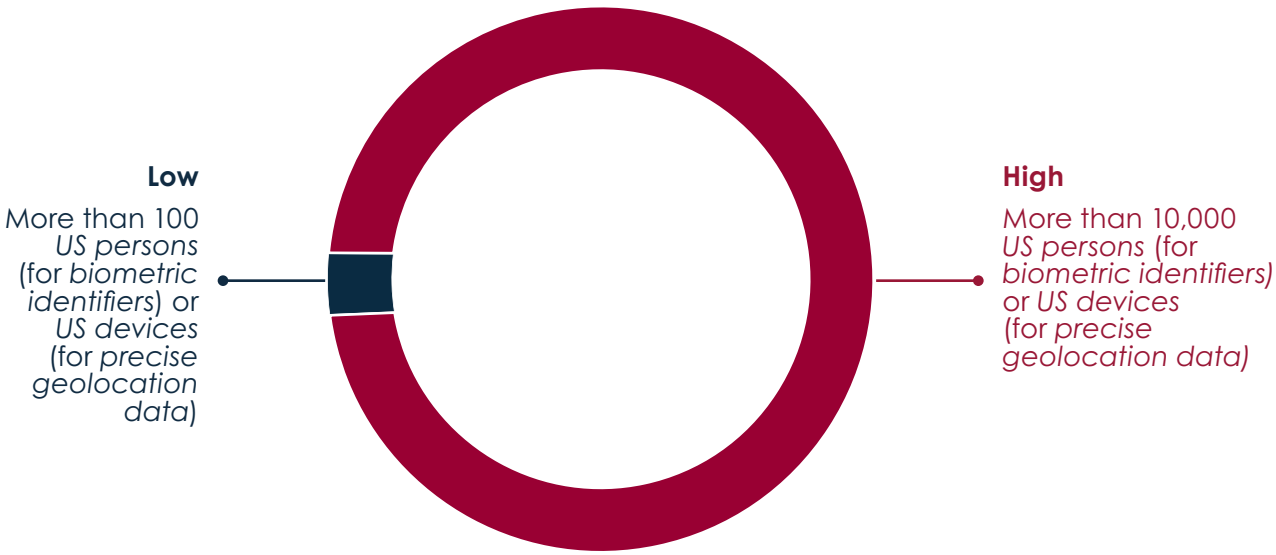
In addition to sensitive personal data, covered data also includes certain government-related data that is likely to include: (1) sensitive personal data marketed as linked or linkable to current or recent former employees or contractors, or former senior officials, of the federal government, including the intelligence community and military and (2) geolocation data that is linked or linkable to certain sensitive locations within geofenced areas that DOJ will specify on a public list.

In most instances, to fall within the new rules a transaction would need to exceed certain bulk volumes defined by DOJ. While these thresholds will be refined as the rulemaking process progresses, DOJ indicates it is considering thresholds within the following ranges:

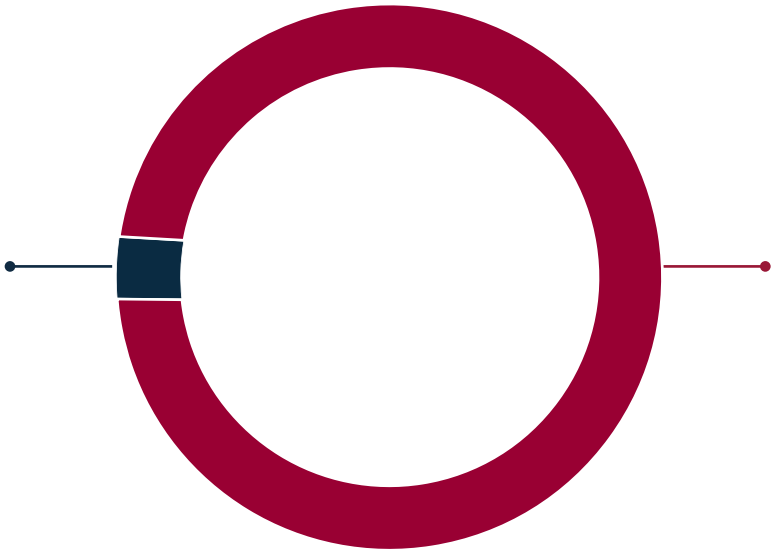
Human Genomic Data



Biometrics Identifiers



Precise Geolocation Data



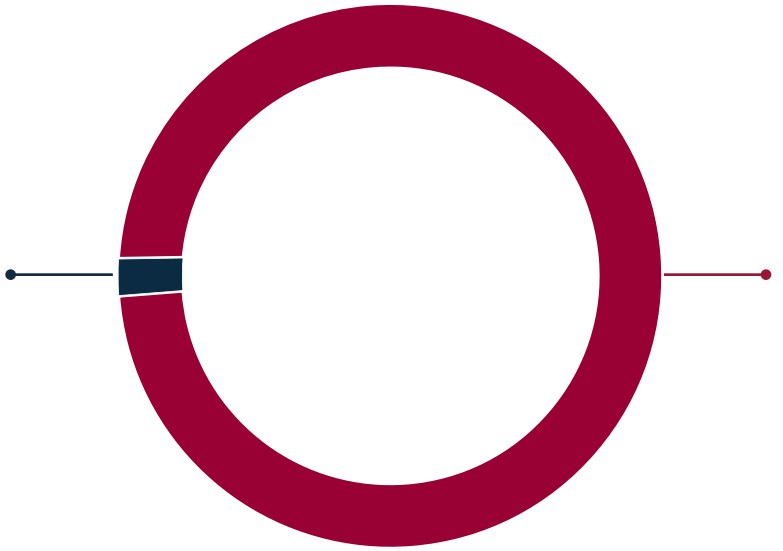
Low

More than 100 *US persons* (for *biometric identifiers*) or *US devices* (for *precise geolocation data*)

High

More than 10,000 *US persons* (for *biometric identifiers)* or *US devices* (for *precise geolocation data)*

Personal Health Data

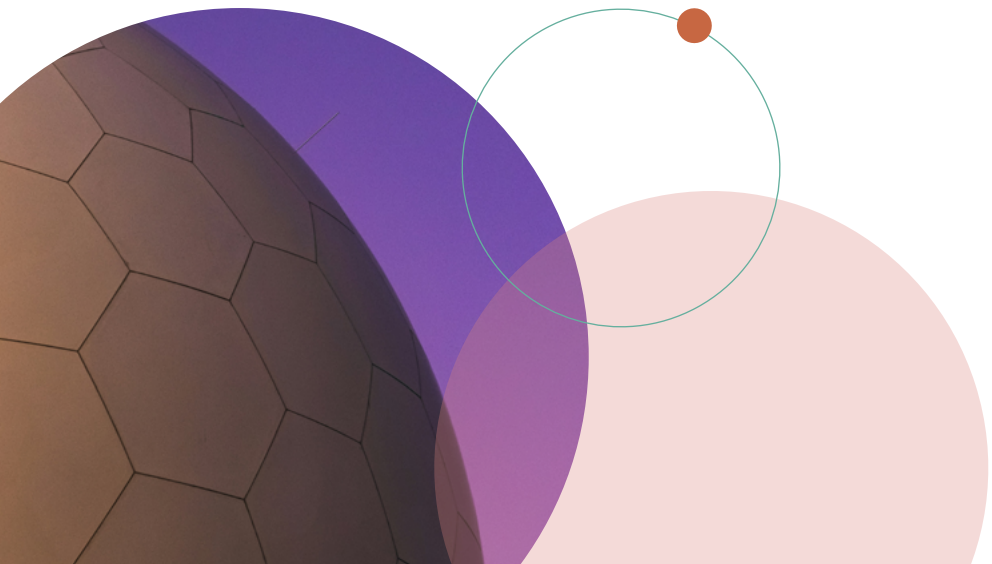


Low

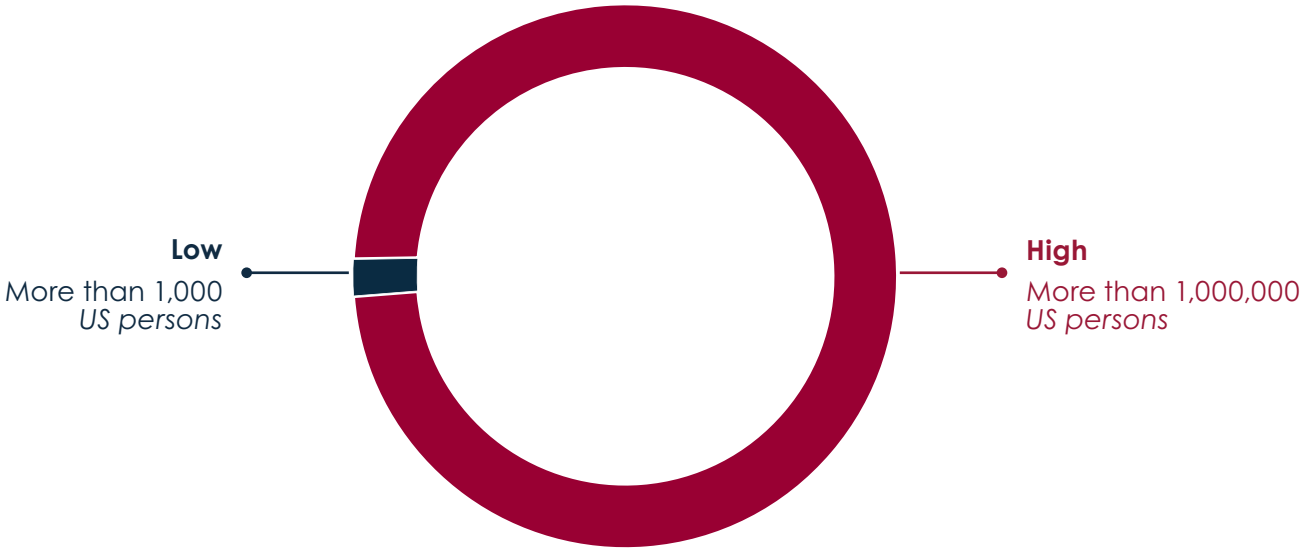
More than 1,000 *US persons*

High

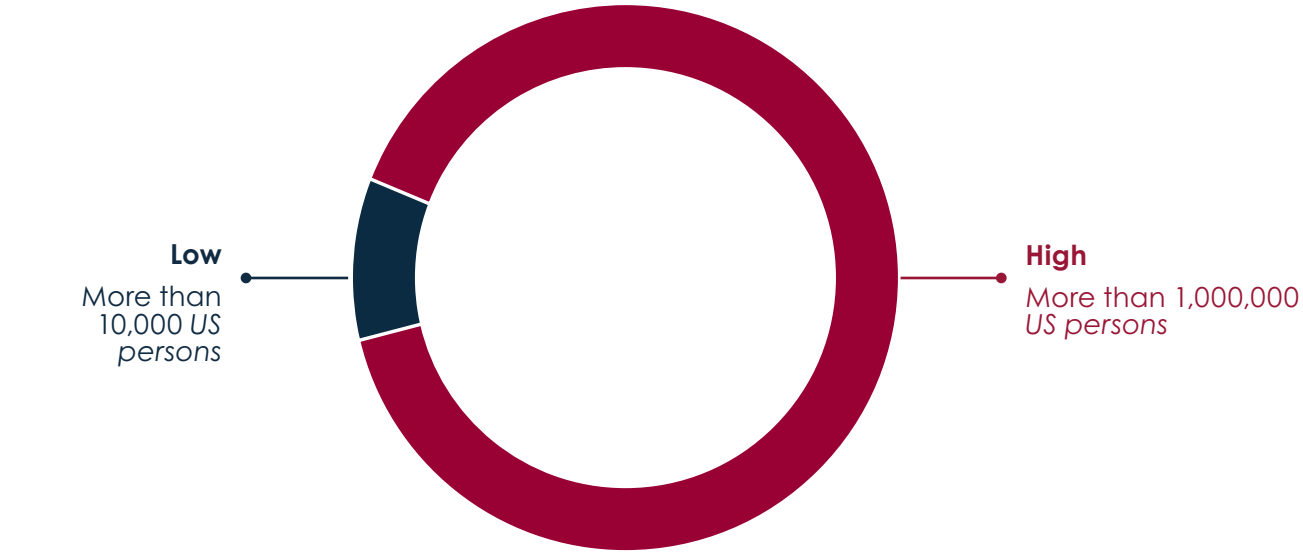
More than 1,000,000 *US persons*



Personal Financial Data



Covered Personal Identifiers



These ranges are relatively low and, particularly if DOJ uses the lower end of these ranges, a significant number of companies could be covered by the new regime.

Importantly, the bulk data thresholds do not apply to US Government-related data, which would be regulated at any level and can include, among other categories, data that can be linked to current or former contractors or employees of the federal government.

B. PADFAA

PADFAA prohibits data brokers from selling, licensing, renting, trading, transferring, releasing, disclosing, providing access to, or otherwise making available personally identifiable sensitive data (the "Covered Activities") of a person residing in the United States to any foreign adversary country (FAC) or any entity that is controlled by a FAC.

Personally identifiable sensitive data includes "any sensitive data that identifies or is linked or reasonably linkable, alone or in combination with other data, to an individual or a device that identifies or is linked or reasonably linkable to an individual."[68] The statute sets forth numerous categories of sensitive data, including: certain health information; certain financial information; biometric information; genetic information; precise geolocation information; private communications content, such as emails, texts, messages, voice communications, and certain associated metadata; account or device credentials; certain demographic information; information identifying an individual's online activities over time and across websites or online services; and information about a minor.

Although the statute bars a wide array of Covered Activities and covers a sweeping range of data, it only applies to a narrowly defined group of "data brokers," which are entities that:

- undertake, for valuable consideration, one or more of these Covered Activities with respect to the data of persons residing in the United States;
- do not collect that data directly from those persons; and
- provide the data to another entity that is not acting as a service provider.

Numerous companies are considered "service providers" under the law. A service provider is an entity that collects, processes, or transfers data on behalf of, and at the direction of, either an individual or entity, which is not a FAC or controlled by a FAC, or a governmental entity. Thus, many entities that engage in the Covered Activities with respect to personally identifiable sensitive data will not be data brokers under the law because the entity receiving the data qualifies as a service provider.

Additionally, the law specifically excludes certain types of entities from the definition of data broker. These include entities that: transmit data, including communications, of a person residing in the United States at the request or direction of that person; provide, maintain, or offer a product or service with respect to which personally identifiable sensitive data, or access to such data, is not the product or service; report or publish news or information of public interest; report, publish, or otherwise make available news or information that is available to the general public such as information from a book, magazine, television program, or a public website; or act as a service provider.

FACs include China, Russia, North Korea, and Iran. One of the following must apply for an entity to be within the control of a FAC:

- Criteria A – A foreign entity with its domicile, headquarters, or principal place of business in a FAC (including an entity that is organized under the laws of a FAC).
- Criteria B – An entity which is at least 20 percent owned, directly or indirectly, by a foreign entity or combination of foreign entities that fall within Criteria A.
- Criteria C – An entity subject to the direction or control of a foreign entity described in Criteria A or B.

These criteria encompass US entities as Criteria B and C are not restricted to foreign entities.

C. Comparison between PADFAA and EO 14117

PADFAA differs in numerous ways from the Biden administration's approach in EO 14117. First, the law only applies to data brokers while EO 14117 and the ANPRM applies to data brokers plus numerous other actors. Second, the executive order and PADFAA diverge on which agency has authority over the sensitive data issue. EO 14117 gave authority over the issue to the DOJ, which is moving forward with the rulemaking process, led by DOJ's National Security Division. In contrast, PADFAA provides the FTC with enforcement authority as part of the FTC's general authorities over unfair or deceptive acts or practices under the FTC Act. Third, in most cases, the ANPRM would only apply to a data transaction that exceeds certain bulk data volumes defined by DOJ. In contrast, PADFAA applies regardless of how much data is made available to an FAC or an entity controlled by an FAC. Fourth, the ANPRM and PADFAA adopt different criteria to qualify as an entity that cannot receive data from a US data broker. For example, unlike the ANPRM, PADFAA prohibits a data broker from transferring data to an entity that is only 20 percent, directly or indirectly, owned by an entity domiciled in a FAC.

These are just a few of the differences between PADFAA and the ANPRM. Given the overlap and potential conflicts between the new statute and the ANPRM, the path forward for the DOJ's ANPRM is somewhat unclear.

68 Protecting Americans' Data from Foreign Adversaries Act of 2024, Section 2(c)(5), Pub. Law No. 118-50.

D. Implications for AI companies and companies using AI

Regardless of the scope of the final restrictions, the AI industry is likely to be significantly impacted given the importance of using vast quantities of data to train AI models and the ability of AI models to review data to identify trends and make connections between seemingly unlinked data points. The restrictions are likely to present a number of compliance challenges for AI companies, many of which operate on a global basis and pool talent from leading AI researchers located around the world. AI companies will likely need to implement compliance procedures to ensure they have a detailed and accurate understanding of the data used in training their models and the individuals and entities that have access to that data. This may involve complex data mapping exercises, working with data vendors and brokers to understand the precise composition of various data sets, and implementing stringent controls on access to certain data.

At least under EO 14117, certain data sets, including those comprised solely of public information may fall outside of the rules. That could be a particularly important carveout for many companies using data scraped from various public sources. As in other contexts, however, it may be difficult in practice to confirm that a data set only contains such public data unless the company using the data was itself the entity that compiled the data or is able to obtain detailed information from its vendor. For AI models that are fine-tuned using more precise, industry-specific data, the public information carveout could be less helpful. PADFAA does not contain the same carveout from the definition of sensitive data.

Under EO 14117, DOJ is unlikely to require companies to adopt compliance programs in this area. However, in keeping with other national security regimes it seems likely to strongly encourage the adoption of risk-based compliance programs for affected entities and may treat the absence of a compliance program as an "aggravating factor" should a violation occur.

VII. Trade Secret Theft and Disruptive Technology Strike Force

On February 16, 2023, DOJ and Commerce, in coordination with the Federal Bureau of Investigation (FBI) and the Department of Homeland Security's Homeland Security Investigations (HSI), launched the Disruptive Technology Strike Force to "target illicit actors, strengthen supply chains and protect critical technological assets from being acquired or used by nation-state adversaries."[69]

In announcing the new strike force, the DOJ cited a number of sensitive technologies including, "supercomputing and exascale computing, artificial intelligence, advanced manufacturing equipment and materials, quantum computing, and biosciences."[70] The strike force is co-led by the Assistant Attorney General for National Security at DOJ and the Assistant Secretary for Export Enforcement in Commerce's Bureau of Industry and Security (BIS), and it focuses on "nation-state adversaries" including China, Iran, Russia, and North Korea, among others. The strike force focuses on both criminal and civil enforcement of export controls.

Since the strike force's establishment, it has been actively pursuing enforcement actions against persons violating US law and seeking to steal sensitive technology, including cases involving AI, semiconductor technology, and a variety of other sensitive technology, software, and equipment. With respect to AI, on March 6, 2024, DOJ announced the arrest of a Chinese national residing in California for allegedly stealing AI-related trade secrets from Google.[71] As described in DOJ's press release, the defendant "transferred sensitive Google trade secrets and other confidential information from Google's network to his personal account while secretly affiliating himself with PRC-based companies in the AI industry."[72] In announcing the arrest, Attorney General Merrick Garland stated, "The Justice Department will not tolerate the theft of artificial intelligence and other advanced technologies that could put our national security at risk" and Deputy Attorney General Lisa Monaco added, "The Justice Department will relentlessly pursue and hold accountable those who would siphon disruptive technologies – especially AI – for unlawful export."

Given the sensitivity of AI from a national security perspective, and the geopolitical and economic incentives for foreign adversaries to steal AI trade secrets, AI-related investigations and enforcement will likely remain a focus of the task force for the foreseeable future.

69 US Dep't of Justice, Press Release, *Justice and Commerce Departments Announce Creation of Disruptive Technology Strike Force* (Feb. 16, 2023), https://www.justice.gov/opa/pr/justice-and-commerce-departments-announce-creation-disruptive-technology-strike-force.

70 *Id.*

71 US Dep't of Justice, Press Release, *Chinese National Residing in California Arrested for Theft of Artificial Intelligence-Related Trade Secrets from Google* (Mar. 6, 2024), https://www.justice.gov/opa/pr/chinese-national-residing-california-arrested-theft-artificial-intelligence-related-trade.

72 *Id.*

VIII. Committee on Foreign Investment in the United States

The Committee on Foreign Investment in the United States (CFIUS) is an interagency committee chaired by the Secretary of the Treasury that is authorized to review certain transactions involving foreign investment in the United States to determine the effect of such transactions on the national security of the United States.

CFIUS has long been focused on the semiconductor industry and on companies with significant quantities of sensitive personal data. That focus will only be heightened going forward as such industries form the critical building blocks of AI, in addition to being sensitive for national security reasons in their own right. While AI models and other AI software have not historically been as heavily scrutinized as those building blocks, they are becoming increasingly scrutinized and the Biden administration has made clear that AI should be a top focus for CFIUS.

A. CFIUS role and authority

CFIUS has the authority to review three types of transactions between a US business and a foreign person: (1) control transactions, (2) certain non-controlling investments, and (3) certain real estate transactions.

A covered control transaction is a transaction that could result in "control" over a "US business" by a "foreign person." Therefore, any US business involved in AI in which a foreign person was taking a controlling interest would be subject to CFIUS jurisdiction. "Control" is broadly defined and frequently does not require the acquisition by the foreign person of a majority interest in the US business. CFIUS regulations specify that minority interests that allow a foreign person "to determine, direct, or decide important matters affecting" the US business may confer control.[73]

CFIUS can also review certain non-controlling investments in US businesses that:

1. produce, design, test, manufacture, fabricate, or develop one or more "critical technologies;"
2. own, operate, manufacture, supply, or service "critical infrastructure;" or
3. maintain or collect "sensitive personal data" of US citizens that may be exploited in a manner that threatens national security.[74]

US businesses that fall into one of these three categories are referred to as "TID businesses" ("T" for technology, "I" for infrastructure, and "D" for data).

To be covered, a non-controlling investment must provide:

1. access to any "material nonpublic technical information" in the possession of the US business;
2. membership or observer rights on, or the right to nominate an individual to a position on, the board of directors or equivalent governing body of the US business; or
3. any involvement, other than through voting of shares, in substantive decision-making of the US business regarding sensitive data, critical technology, or critical infrastructure.[75]

Determining whether a transaction qualifies as a covered non-controlling investment requires a more precise understanding of what constitutes "critical technologies," "critical infrastructure," and "sensitive personal data." "Critical technologies" are defined as (1) items on the United States Munitions List, (2) many items on the Commerce Control List,[76] (3) certain nuclear equipment; (4) certain agents and toxins, or (5) "emerging and foundational technologies" controlled under the Export Control Reform Act of 2018 (ECRA).[77]

"Critical infrastructure" is generally defined as systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating impact on national security.[78] CFIUS regulations provide a detailed list of covered critical infrastructure.[79] Examples include certain internet protocol networks, telecommunication services, internet exchange points, submarine cable systems and landing facilities, financial market utilities, and rail lines that service Department of Defense (DOD) installations, among others.[80] To be considered a critical infrastructure company, a US business must both be involved in one or more enumerated categories of critical infrastructure and meet

73 *See* 31 C.F.R. § 800.208.

74 31 C.F.R. § 800.248.

75 31 C.F.R. § 800.211.

76 In particular, this includes items on the CCL controlled: "(1) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or (2) For reasons relating to regional stability or surreptitious listening." 31 C.F.R. § 800.215.

77 31 C.F.R. § 800.215.

78 31 C.F.R. § 800.214.

79 *See* 31 C.F.R. § Pt. 800, Appendix A. *See also* 31 C.F.R. § 800.212.

80 31 C.F.R. § Pt. 800, Appendix A

certain "functions" related to the critical infrastructure. These functions typically include activity such as "owning or operating" the critical infrastructure or "manufacturing" certain items related to the critical infrastructure. For example, an entity engaged in the function of "owning or operating" an "Internet protocol network that has access to every other internet protocol network solely via settlement-free peering" would be a critical infrastructure company.

Businesses that engage with "sensitive personal data" are those that maintain or collect, directly or indirectly, the identifiable sensitive personal data of US citizens,[81] which:

1. target or tailor products to sensitive US government personnel or contractors;
2. maintain or collect data on more than 1 million individuals; or
3. have a demonstrated business interest in collecting data on more than 1 million individuals and that data is a part of the US business's primary products or services.

Sensitive data is defined to include 10 categories of data maintained or collected by US businesses and includes, for example, certain types of financial information, health information, nonpublic electronic communications, and geolocation data, among other categories.[82]

B. CFIUS jurisdiction over AI-related transactions

Taken together, the existing regulations provide CFIUS with broad authority to review transactions involving AI companies, including control and non-control transactions. As noted above, any control transaction involving AI would be covered by CFIUS rules, and there are several ways an AI company could be considered a TID US business, subjecting it to CFIUS jurisdiction over non-controlling investments.

First, an AI company could qualify as a "critical technology" company. As discussed above, AI software and hardware may be included on the CCL, potentially falling into an ECCN qualifying as "critical technology," or could be included on the USML. Second, an AI company could also qualify as a "sensitive personal data" company. Since vast amounts of data are needed to train AI models, companies engaged in such training may possess data that qualifies as "sensitive personal data" under the criteria set out above. This is more likely to be the case with respect to companies whose AI models are geared towards use in certain industries, such as healthcare, finance, etc., that would likely be trained using sensitive personal data, but could apply to more general models as well. It could also include companies engaged in fine-tuning existing AI models by training them for specific purposes that requires sensitive personal data. Thus, there are multiple avenues through which companies involved in AI could become subject to CFIUS jurisdiction.

In most instances, CFIUS is a voluntary process, meaning parties elect to file to obtain safe harbor from CFIUS later interfering in a deal, including, in the worst-case scenario, ordering a closed transaction to be unwound. It is important to note, however, that in certain cases a pre-closing mandatory CFIUS filing may be required, particularly for critical technology companies and TID transactions involving foreign government-owned entities. The penalty for failing to make such a filing is a fine up to the total value of the transaction.

C. Biden administration CFIUS executive order

On September 15, 2022, President Biden issued an Executive Order (EO) entitled *Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States.*[83] The EO is the first since CFIUS was established in 1975 to "provide formal Presidential direction on the risks that the Committee should consider when reviewing a covered transaction" for its impact on US national security.[84]

The EO elaborates on certain existing factors that CFIUS is statutorily required to consider, and directs the Committee to consider certain additional national security factors in its reviews. In particular, the EO directs CFIUS to consider five factors: (1) the resilience of critical US supply chains; (2) US technological leadership; (3) investment and acquisition trends in a given industry; (4) cybersecurity risk; and (5) access to US persons' sensitive data.

Of the five factors in the EO, the most pertinent with respect to AI is the second factor: the effect of the transaction on US technological leadership (although the other factors could also apply in certain circumstances). Specifically, this factor directs CFIUS to consider "[a] given transaction's effect on US technological leadership in areas affecting US national security, including but not limited to microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy, and climate adaptation technologies" (emphasis added).[85] It further instructs the Committee to consider "whether a covered transaction could reasonably result in future advancements and applications in technology that could undermine national security, and whether a foreign person involved in the transaction has ties to third parties that may pose a threat to US national security."[86]

81 S31 C.F.R. § 800.248(c).

82 Genetic information is also included in the definition regardless of whether it falls into one of the three enumerated categories above. 31 C.F.R. § 800.241.

83 *See* Exec. Order 14083, 87 FR 57369 (Sep. 15, 2022), https://www.federalregister.gov/d/2022-20450.

84 *President Biden Signs Executive Order to Ensure Robust Reviews of Evolving National Security Risks by the Committee on Foreign Investment in the United States, White House* (Sept. 15, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/15/fact-sheet-president-biden-signs-executive-order-to-ensure-robust-reviews-of-evolving-national-security-risks-by-the-committee-on-foreign-investment-in-the-united-states/.

85 *Id.*

86 *Id.*

Given that AI is widely perceived to be central to US technological leadership and competitiveness (now and in the future), the explicit emphasis that the EO places on AI strongly suggests that CFIUS will examine AI-related transactions with a high degree of scrutiny. Similarly, microelectronics (e.g., semiconductors) are seen as crucial to US national security both in their own right and as essential to training AI models. Because AI technology itself, as well as the cutting-edge semiconductors used to train models, are poised to develop rapidly in the coming years, a transaction involving either "could reasonably result in future advancements and applications in technology that could undermine national security."[87]

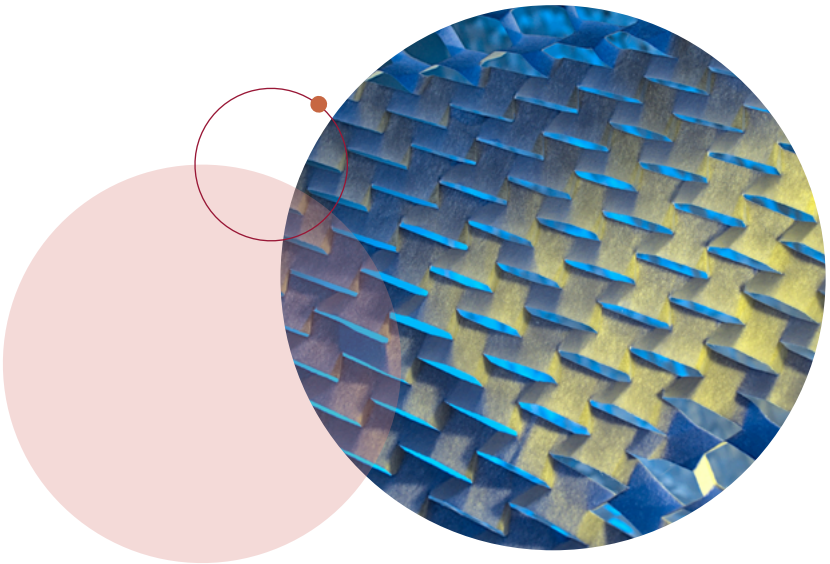
D. CFIUS case studies

CFIUS is typically a confidential process and CFIUS reviews only become public if they are disclosed by the parties, for example in securities filings, or if the president orders a divestment or similar action. To date, there are few publicly known instances of CFIUS blocking or imposing onerous mitigation on AI-related transactions (although that seems likely to change going forward). However, CFIUS has a long history of scuttling deals involving the key AI building blocks of data and advanced semiconductors.

With respect to cases involving companies possessing sensitive data, some of the most notable cases include the CFIUS review of the acquisition of LGBTQ dating app Grindr by the Chinese firm Beijing Kunlun Tech,[88] and the review of the acquisition of online healthcare service PatientsLikeMe by iCarbonX, a Chinese digital healthcare start-up backed by Chinese technology giant Tencent.[89] In both cases, CFIUS forced the Chinese investor to divest its interest in the US company because the transaction parties were not able to sufficiently mitigate the Committee's concerns regarding the potential exploitation of the sensitive personal data. The use of social media platforms' handling of sensitive data and potential use of AI-based algorithms for illicit purposes has also been a focus of CFIUS. These cases demonstrate the difficulty faced by US companies that possess large amounts of sensitive personal data in overcoming CFIUS concerns related to exploitation of that data by a foreign investor.

With respect to semiconductors, CFIUS has a long history of active involvement in the industry, including the proposed acquisition of Fairchild Semiconductor International by China Resources Microelectronics Ltd. and Hua Capital Management Co Ltd.;[90] the attempted acquisition of US semiconductor giant Qualcomm by Broadcom;[91] and the planned acquisition of Magnachip Semiconductor Corporation by the Chinese investment firm Wise Road Capital Ltd.[92]

CFIUS's past history with respect to semiconductors and sensitive personal data, coupled with the new focus on AI outlined in President Biden's EO, suggest CFIUS will heavily scrutinize transactions involving AI companies and companies outside the AI industry that happen to use AI to support their business pursuits.



87 *Id.*

88 *See, e.g.,* Carl O'Donnell, Liana B. Baker and Echo Wang, *Exclusive: Told U.S. security at risk, Chinese firm seeks to sell Grindr dating app, Reuters* (Mar. 27, 2019), https://www.reuters.com/article/us-grindr-m-a-exclusive/exclusive-told-u-s-security-at-risk-chinese-firm-seeks-to-sell-grindr-dating-app-idUSKCN1R809L.

89 *See, e.g.,* Christina Farr & Ari Levy, *The Trump administration is forcing this health start-up that took Chinese money into a fire sale,"* CNBC (Apr. 4, 2019), https://www.cnbc.com/2019/04/04/cfius-forces-patientslikeme-into-fire-sale-booting-chinese-investor.html.

90 *See, e.g.,* Diane Bartz and Liana B. Baker, *Fairchild rejects Chinese offer on U.S. regulatory fears, Reuters* (Feb. 16, 2016), https://www.reuters.com/article/idUSKCN0VP1O7/.

91 *See, e.g.,* Kate O'Keeffe, *Trump Orders Broadcom to Cease Attempt to Buy Qualcomm,* Wall Street Journal (Mar. 13, 2018), https://www.wsj.com/articles/in-letter-cfius-suggests-it-may-soon-recommend-against-broadcom-bid-for-qualcomm-1520869867.

92 *Magnachip Semiconductor Corporation* Form 8-K SEC Filing (Jun. 16, 2021), https://investors.magnachip.com/node/12431/html

IX. Outbound Investment Controls

In addition to CFIUS, which controls inbound foreign investment, the Department of the Treasury is in the process of implementing a new rule focused on outbound US investment involving "countries of concern" and certain sensitive sectors, including the AI sector.

On August 9, 2023, the White House issued an Executive Order entitled Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern (EO 14105). The EO establishes a new national security regulatory regime that will prohibit or require the notification of certain investment activity by US persons in named "countries of concern," currently China (including Hong Kong and Macau).

EO 14105 does not restrict all US person investment activity regarding China, and is tailored to focus on specific products, technologies, and capabilities involving: (1) semiconductors and microelectronics (including advanced integrated circuits used to train AI models and supercomputers); (2) quantum information technologies; and (3) artificial intelligence systems with certain military, intelligence, or surveillance end uses.

EO 14105 directs the Secretary of the Treasury to issue regulations requiring US persons to notify Treasury regarding certain transactions and prohibiting US persons from engaging in certain other transactions, where those transactions involve "persons of a country of concern" engaged in specified activities involving "covered national security technologies and products." Such persons are considered "covered foreign persons."

The term "covered national security technologies and products" includes "sensitive technologies and products in the semiconductors and microelectronics, quantum information technologies, and artificial intelligence sectors that are critical for the military, intelligence, surveillance, or cyber-enabled capabilities of a country of concern," as determined by the Secretary. The EO authorizes the Secretary to extend the implementing regulations to prohibit US persons "from knowingly directing transactions if such transactions would be prohibited transactions pursuant to this order if engaged in by a United States person."[93] It also authorizes the Secretary to require US persons to notify Treasury "of any transaction by a foreign entity controlled by such United States person that would be a notifiable transaction if engaged in by a United States person" and to require US persons to "take all reasonable steps to prohibit and prevent any transaction by a foreign entity controlled by such US person that would be a prohibited transaction if engaged in by a US person."[94]

Treasury published an advance notice of proposed rulemaking (ANPRM), describing how the agency is considering crafting the rules and seeking public comments from industry.[95] The ANPRM contains a number of more granular definitions and likely exemptions to the rules, which are beyond the scope of this white paper.

With respect to AI, Treasury is considering requiring notification for US investments in Chinese entities engaged in activities related to software that incorporates an AI system and is designed exclusively or primarily for certain end uses such as cybersecurity, digital forensics, penetration testing, control of robotics systems, surreptitious listening, locating tracking, and facial recognition. Treasury also requested comments on how to shape a prohibition on US investments in Chinese entities engaged in a narrower set of activities related to software that incorporates an AI system and is designed exclusively or primarily for particular end uses with national security implications such as military, intelligence, and mass surveillance.

The new regime will also include requirements with respect to related sectors, including semiconductors and microelectronics. In particular, Treasury is considering prohibiting US investments in PRC entities engaged in the development of electronic design automation software or semiconductor manufacturing equipment; the design, fabrication, or packaging of advanced integrated circuits; and the installation or sale of supercomputers. Treasury is also considering requiring notification for US investments in PRC entities engaged in the design, fabrication, and packaging of less advanced integrated circuits.

While the AI-related components of the ANPRM are relatively narrowly tailored, it may be difficult in practice to determine whether a Chinese company is engaged in activities with AI that have problematic applications. It also seems possible, if not likely, that those restrictions will change over time as AI concerns grow and evolve. At the time of this writing, Treasury has just issued proposed regulations, which are still open for public comment. We will address these proposed rules or, more likely, the final rules in the next version of this white paper.[96] Congress is actively considering a number of legislative proposals to codify and expand upon the restrictions in EO 14105, so it remains an open question how this issue will be addressed in the near term.

93 Exec. Order 14105.

94 *Id.*

95 *Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of Concern,* 88 FR 54961 (Aug. 14, 2023).

96 *Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of Concern,* 89 FR 55846 (Jul. 5, 2024).

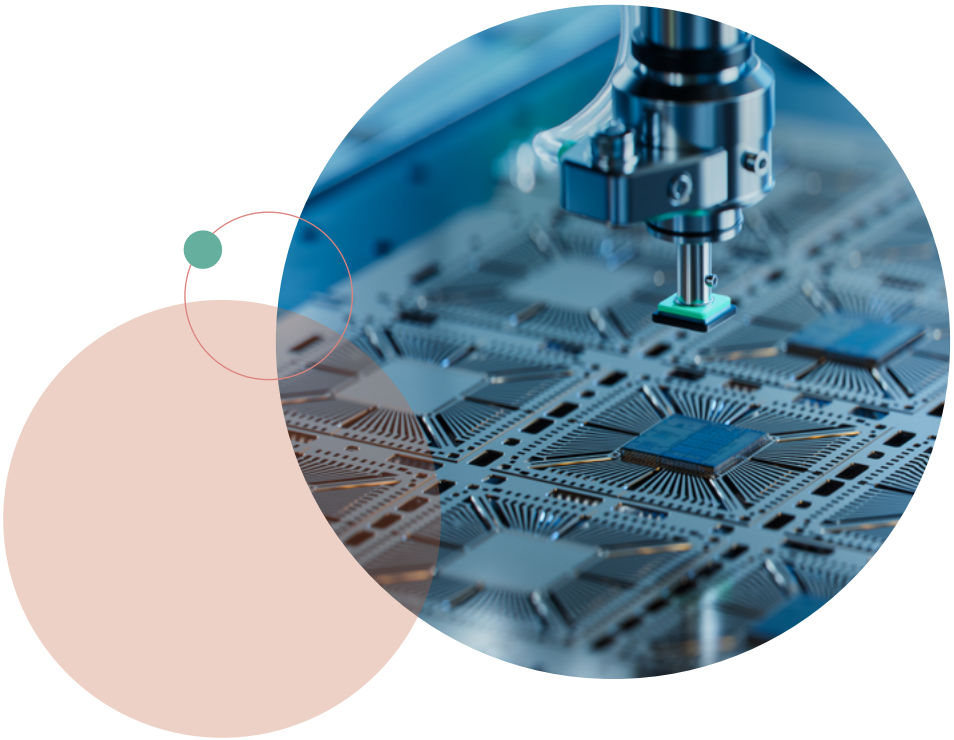
X. Team Telecom

Executive Order 13913 of April 14, 2020 (EO 13913) established the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, which formalized the long-standing interagency review process formerly known, and still often referred to, as Team Telecom.[97]

The process codified by EO 13913 allows the Committee members—DOJ (the chair), DOD, and DHS—to advise the Federal Communications Commission (FCC) on national security and law enforcement considerations relevant to telecommunications licenses implicating certain thresholds of foreign ownership or control. EO 13913 imposed structure, including more predictable timelines for the review and assessment of potential risks, to what had been, historically, a more ad hoc review and advisory process. Principally, the Committee reviews and advises the FCC on transactions implicating new and existing international Section 214 authorizations (relating to provision of international telecommunications service to or from the US) and new and existing submarine cable landing licenses (relating to an international undersea cable that touches US territory).

In some respects, the Team Telecom process shares a similar focus to the ICTS Rule and its implementation of EO 13873 in that they are both aimed at securing the integrity of US telecommunications networks and related infrastructure. Likewise, though entirely separate and independent (despite overlapping membership), certain foreign investment-related national security risks scrutinized by CFIUS can also be a compelling factor for Team Telecom to consider in assessing operational and other security risks relating to certain FCC applications and licenses.

Although AI-related concerns have not been highlighted publicly as a key factor in the Committee's assessment and review process under EO 13913, the growing importance of AI in the telecommunications sector suggests that this will be an expanding area of focus in the future. As telecommunications service providers, including foreign providers seeking to obtain or maintain a Section 214 authorization or submarine cable landing license, seek to leverage AI more prominently in connection with, for example, network management and operations, it seems likely that the Committee will need to assess carefully the potential impact the deployment of such technology may have on US stakeholders and telecommunications infrastructure and whether any identified risks can be mitigated appropriately.



97 *Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector*, Exec. Order No. 13913, 85 FR 19643 (Apr. 8, 2020), https://www.federalregister.gov/d/2020-07530., https://www.federalregister.gov/d/2020-07530

XI. Anti-Money Laundering and Countering the Financing of Terrorism

The rapid advancement of AI is already beginning to have a dramatic impact on anti-money laundering (AML) and countering the financing of terrorism (CFT) efforts by financial institutions around the world. While AI can be used by bad actors to support money laundering and terrorist financing schemes, it is also being used by financial institutions to combat such activity and will likely be a key aspect of AML/CFT compliance programs for most financial institutions going forward.

A. Overview of AML/CFT rules

In the United States, various types of "financial institutions" such as banks, brokers and dealers in securities, and money services businesses, among many others, are required to comply with AML/CFT rules promulgated by the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN). The Bank Secrecy Act (BSA) is the federal statute underpinning most of FinCEN's rules. Those rules impose a range of requirements, such as creating internal policies and procedures designed to prevent the financial institution from being used for illicit financial transactions, conducting customer due diligence, and identifying and reporting suspicious activity, to name just a few. While FinCEN rules are in some cases quite granular and precise, in other cases FinCEN requires a financial institution's program to be appropriately "risk-based" and expects financial institutions to understand the specific risks associated with their business and implement measures to mitigate those risks. Financial institutions that fail to implement appropriate risk-based compliance programs or fail to detect and report on illicit financial activity can be subject to significant civil monetary or even criminal penalties.

B. Current and future uses of AI by financial institutions

By analyzing vast amounts of data in near real time, AI can identify patterns of transactions indicative of money laundering or terrorist financing that might be missed by traditional methods. Transaction monitoring has typically been executed by rules-based systems in which humans program software to flag transactions that violate certain pre-set rules. For example, such software might be programmed to flag users sending transactions over a set dollar threshold or users that initiate a set number of transactions in a short time period. While rules-based software can be very effective in certain scenarios, it inherently relies on humans to know the money laundering typologies to search for and to program those typologies into the software via set rules. This means such software may be behind on new typologies, use rules with inadvertent gaps or loopholes, or have errors in how rules are set. By contrast, AI systems can learn the typologies by studying data, identifying new typologies that may not have been known to or readily identifiable by humans involved in AML/CFT compliance. Use of AI for transaction monitoring should allow compliance programs to identify a greater quantity of suspicious activity, while reducing false positives. In addition, AI may also be helpful for conducting risk assessments, preparing and filing reports, and conducting customer due diligence, among other use cases.

While AI can offer a significant advantage to financial institutions in combatting financial crime, its use is not without challenges. One example is the issue of "explainability" and the fact that many AI models are "black boxes" where it is impossible or difficult to determine precisely how the model generated a given answer. When making important decisions such as whether to close an account or report a user's activity to law enforcement, it is important to have a precise understanding of why a given user or given transaction was flagged by an AI model. Similarly, when filing a suspicious activity report (SAR) under the BSA, it is necessary for a financial institution to be able to explain in the SAR why the transaction is suspicious.

Despite those challenges, AI tools are becoming increasingly common and it is possible that, over time, regulators will effectively require use of AI tools, finding AML compliance programs not appropriately "risk-based" in their absence. This has happened with other IT tools such as blockchain analytics for digital asset companies, whose use, while not specifically called for in regulations, has become expected by AML examiners for companies offering digital asset-based financial services.

C. Statements from FinCEN and other regulators

The benefits of AI and other emerging technologies to combat money laundering have been explicitly recognized by a number of federal regulators, including in a 2018 statement from FinCEN and four federal bank regulators entitled *Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing.* The statement notes that "[s]ome banks are also experimenting with artificial intelligence and digital identity technologies applicable to their BSA/AML compliance programs" and emphasizes that "[t]hese innovations and technologies can strengthen BSA/AML compliance approaches, as well as enhance transaction monitoring systems."[98]

The statement encourages banks to undertake pilot programs utilizing new technologies and notes that banks should not be subject to "supervisory criticism" even if the pilot program is ultimately unsuccessful. Similarly, it explains that pilot programs that expose gaps in BSA/AML compliance programs "will not necessarily result in supervisory action." The statement offers the example of a bank that decides to test or implement an AI-based transaction monitoring system that identifies patterns of suspicious activity not previously detected by the bank and notes "the Agencies will not automatically assume that the banks' existing processes are deficient."[99]

98 *Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing, Board of Governors of the Federal Reserve System,* Board of Governors of the Federal Reserve System, (Dec. 3, 2018), https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20181203a1.pdf .

99 *Id.*

The statement does reiterate that banks must maintain an effective BSA/AML compliance program and undertake careful evaluation of any new compliance systems before fully transitioning to such new technologies.

FinCEN has also addressed AI as part of its Innovation Hours Program in which it facilitates dialogue with industry on key AML/CFT topics. One of the issues identified during this program is a lack of anonymized financial crimes data, making it challenging for AI providers to "properly train and test" AI models related to financial crimes compliance.[100] FinCEN notes that certain AI providers have addressed these issues, in part, by sharing typologies rather than actual customer and transactional data and by use of aggregate SAR statistics published by FinCEN. (Financial institutions are prohibited from disclosing a SAR or information indicating the existence of a SAR outside the financial institution, which can lead to complexities when working with financial crimes compliance vendors.)

On March 27, 2024, Treasury released a report entitled Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector, the production of which was mandated by the AI EO.[101] While the report is not specifically focused on AML, it touches on many adjacent areas including financial fraud and cybersecurity. It highlights a number of AI-related typologies that can contribute to AML risks such as "AI to mimic voice, video, and other behavioral identity factors that financial institutions use to verify a customer's identity."[102] The report also highlights challenges to using AI for compliance, including insufficient sharing of data between financial institutions.

Federal agencies have issued a variety of other guidance that does not directly address AI, but whose principles can nonetheless be applied to AI. For instance, banking regulators have published *Supervisory Guidance on Model Risk Management and issued a statement entitled Interagency Statement on Model Risk Management for Bank Systems Supporting Bank Secrecy Act/Anti-Money Laundering Compliance*, which explains how the supervisory guidance applies to BSA/AML compliance.[103] The supervisory guidance defines a model as "a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates" – a definition that would likely capture many AI models – and outlines how banks should carry out risk management with respect to their use of models.[104] The supervisory guidance, which is not specific to AML and focuses on model use across a bank's activities, walks through a variety of principles including, among many others, evaluating the conceptual soundness of the model, analyzing model outcomes, defining roles and responsibilities, and developing policies and procedures. The interagency statement then explains how the guidance may apply in the BSA/AML context, including when systems used for AML compliance could be considered models, evolving models to respond to rapid changes in the threat landscape, and the use of third-party models. While the supervisory guidance and interagency statement apply to quantitative models generally (and the supervisory guidance applies to models used for all types of bank activities), financial institutions looking to use AI models to assist in AML/CFT compliance would be wise to consider these documents when integrating AI into their compliance systems.

Finally, the Financial Actions Task Force (FATF), an international AML/CFT standards-setting body, has also published a number of reports focused the use of emerging technologies for AML/CFT compliance, including a 2021 report entitled *Opportunities and Challenges of New Technologies for AML/CFT*.[105] The report highlights that "[t]he increased use of digital solutions for AML/CFT based on Artificial Intelligence (AI) and its different subsets (machine learning, natural language processing) can potentially help to better identify risks and respond to, communicate, and monitor suspicious activity."[106]

100 Innovation Hours Program, *Emerging Themes and Future Role in AML Act Implementation,* (May 2019 - February 2021), Financial Crimes Enforcement Network (Mar. 2021), https://www.fincen.gov/sites/default/files/2021-03/FinCEN%20IH%20Prgm%20Public%20Report%20508C.pdf.

101 *Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector,* Department of the Treasury (Mar. 27, 2024), https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf.

102 *Id.* at 18.

103 *Interagency Statement on Model Risk Management for Bank Systems Supporting Bank Secrecy Act/Anti-Money Laundering Compliance,* Board of Governors of the Federal Reserve System (Apr. 9, 2024), https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20210409a2.pdf.

104 *Id.* at 3.

105 *Opportunities and Challenges of New Technologies for AML/CFT,* Financial Action Task Force (Jul. 2021), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.pdf.

106 *Id.*

XII. OFAC Sanctions

In the US, most economic sanctions are administered by the US Department of the Treasury's Office of Foreign Assets Control (OFAC). OFAC has significant discretion to target actors engaged in conduct that is counter to US foreign policy and national security objectives and has increasingly used its authorities to target actors involved with AI.

A. OFAC basics

Broadly speaking, US sanctions can be divided into "primary" and "secondary" sanctions. Primary sanctions are applicable to transactions and activities with a US nexus, including transactions and activities occurring in the United States or in which US persons (including natural persons and entities) are involved. US secondary sanctions typically apply to conduct undertaken by non-US persons, even if there is no direct US nexus, where the United States government has determined the conduct is counter to a US national security and/or foreign policy interest.

At a conceptual level, it is useful to think of two general categories of primary sanctions: (1) sanctions imposed broadly on specific jurisdictions, and (2) sanctions targeted at specific "persons" (including individuals, entities, and government agencies). Some sanctions programs also target specific sectors or industries.

Jurisdictions currently subject to comprehensive sanctions include Cuba, Iran, North Korea, Syria, the Crimea region of Ukraine, and the so-called Donetsk and Luhansk People's Republics regions of Ukraine. US persons are broadly prohibited from dealing with such jurisdictions, unless a specific exemption or license authorizes the conduct in question. US sanctions on Venezuela and Russia are also extensive, while not as comprehensive as those on the other jurisdictions identified above.

Persons, including individuals, entities, and government agencies can be subject to sanctions under a variety of different sanctions programs and identified on lists published by OFAC or other US government agencies. The most significant of these lists is the Specially Designated Nationals and Blocked Persons List (SDN List). The property and interest in property of parties on the SDN List must be frozen when within the United States or in the possession or control of a US person, and US persons are generally prohibited from dealing with SDNs. As a matter of law, entities owned 50 percent or more by one or more persons on the SDN List are also considered blocked.

Civil liability for sanctions violations is enforced on a "strict liability" basis. This means that any transaction or activity violating US primary sanctions may give rise to penalties even if the person undertaking the activity had no knowledge, or reason to know, of the violation. Criminal penalties may only be imposed for "willful" sanctions violations.

B. OFAC and AI

OFAC has a broad range of authorities that it could use to target AI companies engaged in conduct contrary to US foreign policy or national security interests and has already demonstrated a willingness to take such actions. For example, in December 2021, OFAC announced the inclusion of eight Chinese entities on its Non-SDN Chinese Military-Industrial Complex Companies (NS-CMIC) List for allegedly using biometric surveillance technology to track ethnic and religious minorities in China. The OFAC press release describing the action cites the use of AI software that "could recognize persons as being part of the Uyghur ethnic minority and send automated alarms to government authorities."[107] OFAC has also added a regional Chinese government agency to the SDN List for alleged abuses of the Uyghur population in Northwest China, including for the use of "an artificial intelligence (AI)-assisted computer system that created biometric records for millions of Uyghurs in the Xinjiang region."[108]

A number of other OFAC authorities have not yet been used to target AI companies, but certainly could be in the future. For instance, OFAC is currently charged with implementing a range of executive orders authorizing the blocking (i.e., SDN designation) of persons engaged in malicious cyber-enabled activities, election interference (which could include things such as the creation or dissemination of AI-generated deepfakes), and human rights abuses (such as AI-powered surveillance), to offer just a few examples.

107 *Treasury Identifies Eight Chinese Tech Firms as Part of The Chinese Military-Industrial Complex,* Department of the Treasury (Dec. 16, 2021), https://home.treasury.gov/news/press-releases/jy0538.

108 *Treasury Sanctions Perpetrators of Serious Human Rights Abuse on International Human Rights Day,* Department of the Treasury (Dec. 10, 2021), https://home.treasury.gov/news/press-releases/jy0526.

By contrast, AI is increasingly becoming a tool that can be used to promote sanctions compliance by helping financial institutions and other companies identify customers, counterparties, or transactions that may be subject to sanctions or located in a comprehensively sanctioned jurisdiction. In September 2022, OFAC published Sanctions Compliance Guidance for Instant Payment Systems in which it noted "OFAC is aware of artificial intelligence tools and other innovative compliance solutions, such as those that leverage information sharing mechanisms across financial institutions, which may enhance sanctions screening functions and reduce false positives."[109] It added, "Where appropriate … OFAC encourages the use of such tools and other emerging technologies and solutions to manage sanctions risks that could arise in the context of instant payments."[110]

As AI tools become increasingly prevalent in the compliance space, it is possible OFAC may ultimately come to expect the use of AI in sanctions compliance, at least for financial institutions and larger international companies.

109 *Sanctions Compliance Guidance for Instant Payment Systems,* Department of the Treasury (September 2022), https://ofac.treasury.gov/media/928316/download?inline.

110 *Id.*

XIII. Government Contracts

Federal agencies are increasingly focusing on ways to use and manage AI through contracting. To date, agencies have mostly issued policy statements and guidelines. However, they have announced how they expect to procure AI and support associated research and development, as well as how they expect contractors to use AI when performing work on behalf of the US Government.

A. Office of management and budget memorandum

As required by the AI EO, the Office of Management and Budget (OMB) issued a memorandum on March 28, 2024 that provides guidance to federal agencies on the use of AI.[111] At the same time, OMB issued a request for information on ways in which the US government can more responsibly and effectively procure AI.

The memorandum applies to all executive agencies and independent establishments other than members of the intelligence community. The memorandum also covers most AI developed, used, or procured by or on behalf of a covered agency, subject to key exceptions for: (1) AI used to carry out basic or applied research unrelated to the development of an AI application and (2) national security systems, which are either classified or used for intelligence activities, cryptologic activities related to national security, or command and control of military forces, or as an integral part of a weapon or weapon system or as an item that is critical to the direct fulfillment of military or intelligence missions.[112] Thus, the memorandum does not cover AI used in earlier-stage research and development projects and most AI use cases in DOD and other national security agencies relating to warfighting or intelligence missions.

Under the memorandum, each federal agency other than DOD that uses AI outside of national security systems needs to provide OMB with an annual inventory of its AI use cases. Each agency needs to identify whether its use cases are "safety-impacting" or "rights-impacting," which respectively refer to AI that provides outputs serving as a principal basis for a decision or action with a significant effect concerning: (1) a specific individual's or entity's civil rights, liberties, or privacy, equal opportunities, or access to critical government resources or services and (2) safety of any human life or well-being, climate or environment, critical infrastructure, or strategic assets or resources, including sensitive or classified federal government information. Subject to exceptions under applicable law and policy, each agency needs to release a public version of its annual use cases on its website.

Agencies are also required to share AI software code, including models and weights, developed (1) by their employees, (2) in the performance of a US government contract, or (3) solely with US government funds. Disclosure is required to both other US government agencies and the public subject to a number of exceptions, including restrictions under law or regulation, intellectual property rights, and other contractual commitments. Data sets in an agency's possession or control that would be disclosable under the Freedom of Information Act also need to be made publicly available in a variety of circumstances. In addition, agencies are encouraged to acquire AI code, models, data sets, and enrichment services like labeling in a way that allows for this type of sharing. In practice, however, the exceptions that take into account intellectual property rights and other contractual commitments may limit agency disclosures for most AI resources developed by private industry.

By December 1, 2024, again subject to applicable exceptions and waivers, agencies will also need to adopt minimum practices for "rights-impacting" and "safety-impacting" AI that they use, including requirements to complete detailed AI impact assessments, test AI in real-world contexts and using independent agency components, and provide notice to end-users of agency services about the use of AI. "Rights-impacting" AI will also need to be reviewed for algorithmic discrimination, require notice to affected individuals about the use of AI to reach an adverse decision or action, have a fallback human review and escalation system for appeals, only be used after public consultation, and, where practicable, have an option for the public to opt out of AI functionality.

When procuring AI, the OMB memorandum encourages agencies to seek details about the source and characteristics of data sets - also known as "provenance" - and obtain rights in underlying data sets and improvements, prevent unauthorized use of government data for training, and guard against tailoring of AI to known government test requirements (i.e., by specifically training AI to give correct answers in response to government verification and validation tests). In addition, recognizing the high computational needs of some AI, the OMB memorandum encourages agencies to consider the environmental impact of procured AI services, including carbon emissions and resource consumption from supporting data centers.

As is often the case, state governments will likely adopt similar requirements and guidance with respect to their own procurements. For example, California has already issued new procurement guidelines for generative AI that impose mandatory disclosure requirements when companies offer generative AI to the state government, as well as similar transparency and risk evaluation procedures.[113]

111 *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence,* Office of Mgmt. & Budget (Mar. 2024), https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf.

112 44 U.S.C. § 3552(b)(6).

113 Cal. Dep't of Tech. *et al., State of California GenAI Guidelines for Public Sector Procurement, Uses and Training,* (Mar. 2024), https://www.govops.ca.gov/wp-content/uploads/sites/11/2024/03/3.a-GenAI-Guidelines.pdf.

B. National security systems

Federal national security systems will be subject to a separate memorandum that is currently in process. If prior memoranda are any indication, this separate memorandum will likely set only high-level goals and not prescribe particular ways of using or acquiring AI. Compared to OMB's memorandum for other systems, commentators have expressed concern that the national security memorandum will not place concrete limitations on or require disclosure of how AI is being used.[114]

For now, national security systems are covered by various policy statements, such as the Ethical AI Principles and report on Responsible Artificial Intelligence Strategy and Implementation Pathway issued by DOD.[115] AI systems are also increasingly being supported by national security agencies like DOD, with approximately 70 percent of a major DOD research agency's programs involving AI as of March 27, 2024.[116] In addition, DOD has implemented test bed programs to develop and demonstrate AI in a variety of fields, including most prominently with respect to uncrewed autonomous vehicles.[117]

On April 15, 2024, the National Security Agency (NSA) also released guidance on securely deploying AI systems, which supplements previous intelligence community guidance focused on AI security.[118] The NSA emphasized the importance of ensuring that a company's general cybersecurity protections extend to its AI systems directly and at network boundaries with AI, and highlighted the need to have heightened protections for model weights, which are susceptible to misuse even within internal networks. The NSA also emphasized the need to establish trusted data sources for training and operation of AI in order to avoid data poisoning or backdoor attacks through AI models, especially given that AI is often developed iteratively based on deployment in real-world contexts. In addition, the NSA noted the importance of using hardened containers, encryption, and zero-trust frameworks when deploying AI systems for real-world use.

Similar to the OMB memorandum, DOD has also implemented a requirement to maintain a non public inventory of its current AI activities and emphasized the need to conduct verification and validation of procured AI solutions. With respect to dual-use foundation models described in the AI EO, DOD may ultimately be reluctant to procure models from companies that do not provide high levels of transparency about AI training, ownership, protection of model weights, and red-team testing as described in the EO.

> Moreover, in practice, DOD has increasingly gone beyond traditional CFIUS, export controls, and foreign ownership, control, or influence considerations (FOCI) to withhold or limit funding for companies that develop critical technologies like AI if they have ties to countries of concern, such as a limited number of minority owners in China.

With respect to weapon systems, DOD has emphasized the importance of using "human-in-the-loop" or "human-on-the-loop" AI systems that require some form of human control or oversight. However, there is currently no blanket prohibition on acquiring or using entirely autonomous weapon systems.[119] For example, DOD only requires that there be "appropriate levels of human judgment over the use of force," recognizing that the strategic value of some AI systems may be undermined if humans are involved, such as due to delayed response times.[120]

Strategically, DOD is focused on using AI in the national security space for decision advantage across multiple aspects of its operations, including battlespace awareness, logistics, kill chains, and enterprise business operations.[121] DOD has also embraced iterative development of "minimum viable products" that are continually improved over time through real-world use, which coincides with the commercial development cycle of most AI. National security agencies as a whole are recognizing the need to view AI development and adoption, as well as related on-shoring of semiconductor production capacity, as competitive efforts against adversaries in a race to develop new technologies. For example, the National Security Commission on Artificial Intelligence repeatedly characterized China as an AI peer or leader in critical areas to argue for ramping up AI development efforts in the United States.[122]

DOD is also focused on promoting the use of trusted AI in the defense industrial base. On May 22, 2024, DoD began seeking public comment on a variety of issues that will inform an AI Defense Industiral Base Roadmap, including details on potential AI vulnerabilities, work with nontraditional defense contractors, information-sharing, and intellectual property considerations.[123]

114 *See, e.g., Bringing Transparency to National Security Uses of Artificial Intelligence, Just Security* (Apr. 2024), https://www.justsecurity.org/94113/bringing-transparency-to-national-security-uses-of-artificial-intelligence/.

115 *Implementing Responsible Artificial Intelligence in the Department of Defense,"* Dep't of Def. (May 2021), https://media.defense.gov/2021/May/27/2002730593/-1/-1/0/IMPLEMENTING-RESPONSIBLE-ARTIFICIAL-INTELLIGENCE-IN-THE-DEPARTMENT-OF-DEFENSE.PDF; "Responsible Artificial Intelligence Strategy and Implementation Pathway," Dep't of Def. (Jun. 2022), https://www.ai.mil/docs/RAI_Strategy_and_Implementation_Pathway_6-21-22.pdf.

116 *DARPA Aims to Develop AI, Autonomy Applications Warfighters Can Trust,* Dep't of Def. (Mar. 2024), https://www.defense.gov/News/News-Stories/Article/Article/3722849/darpa-aims-to-develop-ai-autonomy-applications-warfighters-can-trust/.

117 *F-16s arrive to be modified for autonomous testing,* Dep't of the Air Force (Apr. 2024), https://www.af.mil/News/Article-Display/Article/3728795/f-16s-arrive-to-be-modified-for-autonomous-testing/.

118 *Deploying AI Systems Securely,* Nat'l Sec. Agency (Apr. 2024), https://media.defense.gov/2024/Apr/15/2003439257/-1/-1/0/CSI-DEPLOYING-AI-SYSTEMS-SECURELY.PDF; *Guidelines for secure AI system development, Cybersecurity and Infrastructure Security Agency et al.* (Nov 2023), https://www.cisa.gov/news-events/alerts/2023/11/26/cisa-and-uk-ncsc-unveil-joint-guidelines-secure-ai-system-development.

119 *Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems,* Congressional Research Serv. (Feb. 1, 2024), https://crsreports.congress.gov/product/pdf/IF/IF11150.

120 DODD 3000.09 (2023).

121 *Data, Analytics, and Artificial Intelligence Adoption Strategy,* Dep't of Def. (Nov. 2023), https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF.

122 *Final Report,* Nat'l Sec. Comm. on Artificial Intelligence (2021), https://reports.nscai.gov/final-report/.

123 FN 89 Fed. Reg. 44,964 (May 22, 2024)

C. Innovative acquisition pathways and agreements

To increase the normally slow speed of procurement, federal agencies are increasingly relying on innovative acquisition pathways and agreements to acquire and support development of AI products and services. For instance, federal agencies have been using broad agency announcements and commercial solutions openings to fund basic and applied research and, at times, prototyping and demonstration efforts.[124] These types of competitions involve offerors submitting disparate explanations of how they would solve a high-level government problem instead of each offeror tailoring their proposals to the same set of government requirements and competing head-to-head.

Similarly, federal agencies have increasingly used non-standard government agreements like "other transaction authority" agreements to fund AI work. If structured properly, these agreements can lead to large-scale follow-on purchases without further competition.[125] Agencies have also issued these "other transaction authority" agreements under consortia that are partially or fully managed by private partners, which is intended to further streamline the funding process.[126] In addition, agencies have turned to prize competitions to influence private development by announcing the availability of funds for the first companies to meet a particular government objective.[127] NIST also recently announced its intent to hold a competition for a new Manufacturing USA institute, which would be sponsored by the US government while being run by one or more private companies, with a focus on bringing together industry, academia, and federal, state, and local governments to use AI to improve resilience of US manufacturing.[128]

D. Data rights

Corresponding to the new focus on AI, national security agencies are grappling with new problems in acquisition posed by the relationship between AI models and data sets. For example, the Defense Innovation Board (DIB) recently noted that DOD faces significant hurdles in obtaining sufficient rights in data sets, which the DIB views as necessary to fully implement DOD's integration of AI into its operations.[129] In effect, the DIB is focused on DOD having access to and rights in AI systems as a whole instead of just AI models that are provided in containerized form or accessed through a cloud service. Other national security agencies can be expected to similarly grapple with this issue and push private companies to provide broader access to AI systems than would normally be granted in the private sector. To address this issue, the DIB made a relatively extreme recommendation of including provisions in the National Defense Authorization Act for Fiscal Year 2025 mandating that DOD obtain rights in (1) data obtained from commercially available, subscription-based platforms, (2) data generated through use of DOD-funded AI technologies, and (3) future modifications to AI data sets and ensembles. In this context, it is likely that DOD and other national security agencies will continue to push for broader rights to use and modify AI systems.

DOD and other national security agencies may also try to leverage mechanisms that are already in place to accomplish this goal. For example, in standard procurement contracts in which the federal government buys a product or service or funds research and development, agencies already have discretion to include "data ordering clauses" to demand access to any data generated in performance of the contract or, for agencies other than DOD, any data that is merely used in performance.[130] As a result, agencies may take the position that they already have authority to demand access to data sets used in operating AI or at least to data set modifications that take place in performing a US government contract.

DOD and other agencies may also take aggressive views on the scope of data that is deemed necessary for operation, training, or maintenance purposes relating to AI products or services provided to the US government. By default, agencies often obtain "unlimited rights" in such data to use it for any purpose.[131] These rights were originally intended to cover things like instruction manuals for hardware. However, DOD and other agencies have repeatedly argued that these rights extend to other types of data, such as technical specifications, engineering drawings, and source code. Based on those prior positions, agencies may aggressively argue that certain data sets or model weights are necessary for operation, training, or maintenance of AI systems and services, thereby giving agencies unlimited rights to use this data for AI systems and services that they procure.

Further, as alluded to by a conspicuous reference in the AI EO's discussion of data access rights for dual-use foundation models, federal agencies could also exercise their rights under the Defense Production Act to demand access to data sets and other technical information relating to AI systems.[132] This mechanism could be used to go beyond data generated or used in performance of a government contract to access, for example, model weights, and algorithms. Recipients of a directive under the Defense Production Act would presumably be entitled to some form of compensation for any corresponding loss in value of their AI systems. Recovering meaningful damages or remuneration may be difficult, however, and would likely involve a lengthy process.

124 10 U.S.C. § 3458; FAR 35.016.

125 10 U.S.C. § 4022.

126 *See, e.g.*, Trade Winds, https://www.tradewindai.com/; Expeditionary Missions Consortium, https://www.emccrane.org/.

127 *See, e.g.*, https://aicyberchallenge.com/.

128 89 FR 18,373 (Mar. 13, 2024).

129 *Building a DoD Data Economy* at 15, Def. Innovation Bd., (2024), https://innovation.defense.gov/Portals/63/20240118%20DIB%20Data%20Economy%20Study_Approved-compressed.pdf.

130 FAR 52.227-16; DFARS 252.227-7027.

131 FAR 52.227-14(b)(1)(iii); DFARS 252.227-7013(b)(1)(v).

132 For example, DOD has been delegated this right under 15 C.F.R. Part 700, which defines covered items as including any "technical information, process, or service" in addition to the supplies and raw resources that are typically subject to the Defense Production Act.

E. Intellectual property

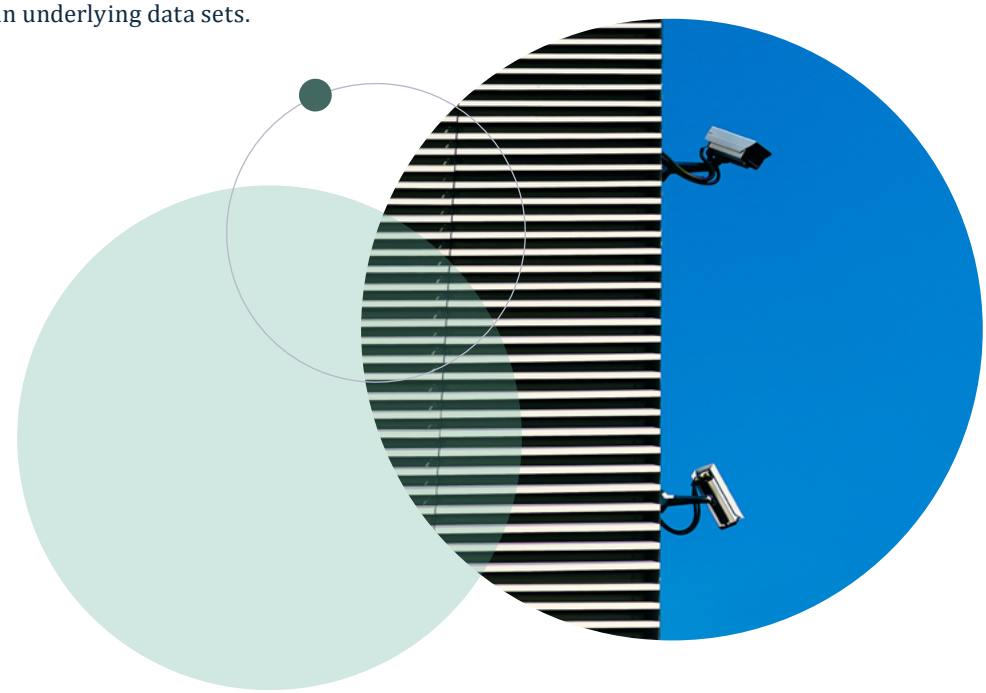
Companies that are familiar with US government contracts should also be aware that traditional protections from liability for intellectual property infringement may not apply to many AI systems. For example, express "authorization and consent" provisions that often make the US government initially liable for infringement under a government contract and prevent its performance from being enjoined only apply to patent infringement, which is less of a concern to AI software providers that often rely on copyright.[133] It may also be difficult for AI companies to argue that the government provided implied "authorization and consent" to permit copyright infringement in performance of a government contract because the government may be able to credibly claim that it did not have sufficient knowledge to provide "authorization and consent" and take on liability for infringement with respect to an AI system with undisclosed model weights, algorithms, and data sets.

F. Personally identifiable information

Separately, companies applying AI systems to personally identifiable information for or on behalf of the US government should be aware that they may be subject to heightened requirements that only apply to the US government and its contractors. For instance, a contractor operating a database controlled by a federal agency that includes personal information that can be retrieved by individual names or identifiers can be subject to the Privacy Act, which treats contractor personnel like federal employees for the purpose of the Act's criminal provisions.[134] As a result, a contractor and personnel that use AI to process a government database with individual identifiers could be subject to heightened liability for unauthorized disclosures, such as those driven by faulty AI outputs or a failure to take sufficient precautions to protect an AI model from inversion attacks that reveal personally identifiable information in underlying data sets.

Additionally, DOD contractors are now subject to a prohibition on selling, licensing, or otherwise transferring personally identifiable information about DOD employees or members of the armed forces received through a government contract, which may be relevant to companies that use contract data to improve their AI models or data sets.[135] As directed by the OMB memorandum, DOD and other agencies may also start prohibiting the use of any contract data for training purposes without agency consent. Even now, many DOD agreements already include a provision prohibiting release of information pertaining to any part of a contract or program related to a contract, which could create difficulties for companies that want to use contract data to improve AI models or data sets.[136]

Interestingly, the OMB memorandum itself and other recent guidance would not do much to protect personally identifiable information that is used in human research. By exempting basic and applied research from coverage under the memorandum unless specifically directed at developing an AI application, traditional clinical trials and social sciences research funded by the US government would not be subject to the memorandum's heightened protections. For example, the National Institutes of Health and its contractors would not be required by the memorandum to disclose when AI is being used to screen patients. They would also not need to worry about whether AI should be managed as "rights-impacting" or "safety impacting," such as when AI is used in connection with patient informed consent or adverse events. These types of issues may ultimately be addressed through updates to existing regulations that cover human research that is supported by the US government.[137]



133 28 U.S.C. § 1498; FAR 52.227-1.

134 5 U.S.C. § 552a(i), (m).

135 10 U.S.C. § 4662.

136 DFARS 252.204-7000.

137 45 C.F.R. Part 46.

XIV. Conclusion

Contrary to much of the public discourse suggesting AI is unregulated by the US government, there are a wide variety of existing and newly created legal regimes that have a significant impact on AI. Those laws apply to AI in various contexts, including, notably, with respect to national security, and it is reasonable to expect legal and regulatory complexity will continue to expand in this area in the future, particularly in connection with the implementation of the AI EO.

Whether a company is developing AI, using AI, or working with one of the key AI building blocks of data or semiconductors, understanding these laws is essential.

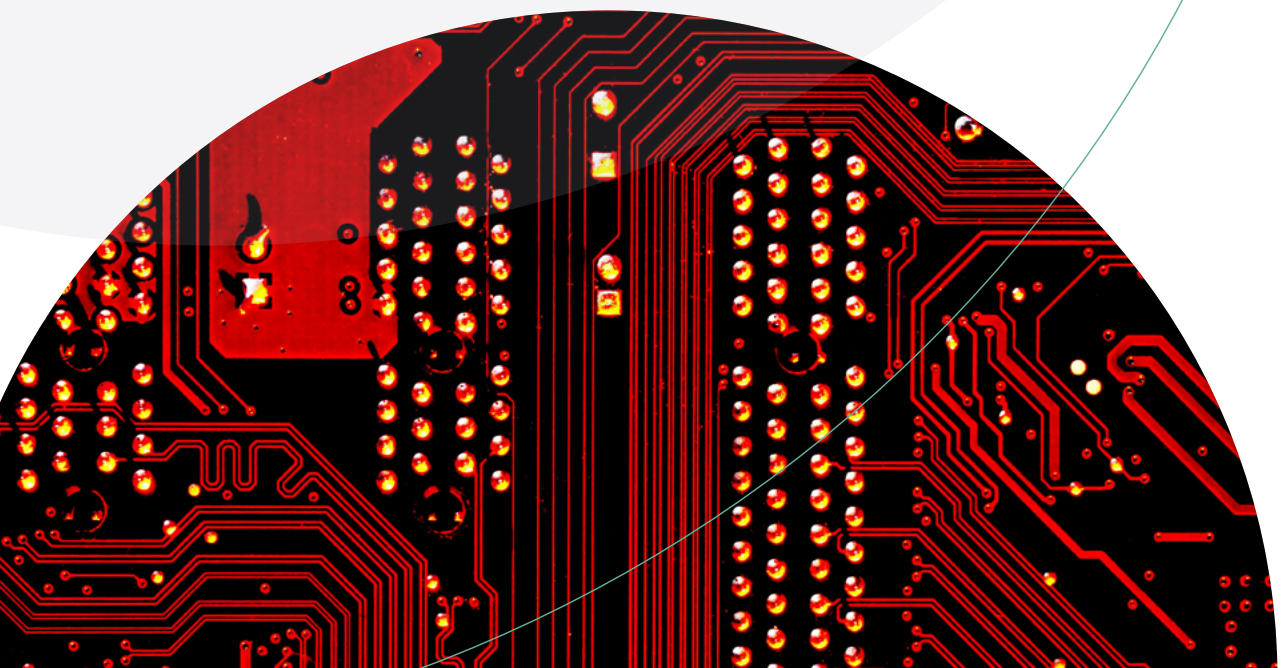
Contrary to much of the public discourse suggesting AI is unregulated by the US government, there are a wide variety of existing and newly created legal regimes that have a significant impact on AI. Those laws apply to AI in various contexts, including, notably, with respect to national security, and it is reasonable to expect legal and regulatory complexity will continue to expand in this area in the future, particularly in connection with the implementation of the AI EO. Whether a company is developing AI, using AI, or working with one of the key AI building blocks of data or semiconductors, understanding these laws is essential.

> For additional information any of the legal regimes discussed above please contact a member of the Steptoe AI or National Security teams.

Lead Authors:
Brian Fleming (Partner, International Regulatory Compliance),
Evan Abrams (Associate, International Regulatory Compliance)

Contributors:
Tyler Evans (Partner, Government Contracts), Tod Cohen (Partner, AI, Data & Digital), Anne-Gabrielle Haie (Partner, AI, Data & Digital), Christopher Forsgren (Associate, International Regulatory Compliance)

Special Thanks To:
Sean Gallagher (Former Analyst, International Regulatory Compliance), Craig Nelson (Paralegal, IP Litigation)



About Steptoe

Steptoe is well-known for integrating legal, strategic policy and advocacy, and pragmatic business considerations to develop effective solutions to regulatory challenges for our clients.

In more than 100 years of practice, Steptoe has earned an international reputation for vigorous representation of clients before governmental agencies, successful advocacy in litigation and arbitration, and creative and practical advice in structuring business transactions. Steptoe has more than 500 lawyers and other professional staff across offices in Beijing, Brussels, Chicago, Hong Kong, Houston, London, Los Angeles, New York, San Francisco, and Washington.

Keeping You Informed

Visit www.steptoe.com to subscribe and stay up-to-date with fast-moving developments.

International Compliance Blog

Get a fresh perspective on global compliance issues, with insights into dynamic fields such as export controls, economic sanctions, and anti-corruption measures.

StepTechToe Blog

StepTechToe is our AI, Data & Digital Regulation blog, which offers up-to-date and seasoned perspectives on the regulatory framework governing digital services.

About the Authors

Brian Fleming
Partner | Washington, DC | bfleming@steptoe.com | Full Profile

Brian Fleming focuses his practice on matters at the intersection of national security and international trade, with an emphasis on economic sanctions, export controls, and foreign direct investment. US and international clients turn to Brian for advice regarding the Committee on Foreign Investment in the United States (CFIUS) process, from pre-transaction risk assessments to preparation of voluntary and mandatory CFIUS filings and management of mitigation agreements. During his time in the National Security Division (NSD) of the US Department of Justice (DOJ), Brian worked closely with senior NSD leadership, as well as the Foreign Investment Review Section (FIRS), to manage DOJ's review of all CFIUS matters and advised on numerous transactions and mitigation proposals across various industries. He uses his government experience, along with his deep understanding of US national security interests and the demands of cross-border global business, to offer practical guidance and strategies for his CFIUS clients.

Evan Abrams
Associate | Washington, DC | eabrams@steptoe.com | Full Profile

Evan Abrams counsels financial institutions, multinational corporations, and individuals on a variety of international regulatory and compliance matters. He regularly advises clients on issues related to anti-money laundering (AML), economic sanctions, export controls, foreign anti-corruption, the Committee on Foreign Investment in the United States (CFIUS), and the Defense Counterintelligence and Security Agency (DCSA). Among other sectors, his practice focuses on emerging technology and financial technology where he leverages his deep understanding of business trends and technological developments to help clients achieve their commercial objectives while complying with complex regulatory regimes.

Steptoe

For more information about Steptoe, the partners and their qualifications, **see www.steptoe.com.**

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising. Images of people may feature current or former lawyers and employees at Steptoe or models not connected with the firm.