GIBSON DUNN

U.S. Commerce Department Poised to Dramatically Expand Compliance Requirements in Key Technology Sectors

Client Alert | February 29, 2024

The Office of Information and Communications Technology and Services of the U.S. Department of Commerce is poised to dramatically expand compliance requirements in key technology sectors with new leadership and proposed new regulations targeting Infrastructure as a Service providers and large AI model training. Since coming into office, the Biden administration has largely continued and expanded efforts to regulate AI and other emerging technologies begun under the Trump administration, and recent actions by the U.S. Department of Commerce ("Commerce") signal that U.S. Infrastructure as a Service ("IaaS")providers and their resellers will soon face a host of new compliance requirements concerning their customers and ultimate end-users. Commerce recently announced the appointment of Elizabeth Cannon as the first Executive Director of the Office of Information and Communications Technology and Services ("OICTS"), signaling a renewed focus on the information and communications technology and services ("ICTS") sector. For several years, Commerce has worked to stand up OICTS to implement a series of executive orders ("EOs") issued by the Trump and Biden administrations aimed at securing the telecommunications supply chain,[1] addressing malicious cyber-enabled activity,[2] protecting the sensitive data of U.S. citizens,[3] and providing guardrails on the use and development of AI.[4] Finalizing regulations implementing these varied EOs has proven a difficult task, as Commerce, along with partner government agencies, continue to develop measures designed to address pressing national security concerns while simultaneously avoiding stifling the innovation necessary to develop emerging technologies. Early in this effort, Commerce developed regulations permitting the Secretary of Commerce ("Secretary") to block certain information and communications technology or service transactions involving "foreign adversaries." These regulations became effective in March 2021, implementing Trump era EO 13,873. The Biden administration quickly followed suit after taking office, issuing a pair of EOs aimed at protecting the sensitive data of U.S. citizens (EO 14,034) and providing guardrails for the development and use of AI (EO 14,110), in addition to regulations expanding the Secretary's discretion to block transactions involving "connected software application" and foreign adversaries. More recently, Commerce announced an advance notice of proposed rulemaking to solicit public comment on similar restrictions targeting transactions involving "connected vehicles," a term whose definition has yet to be defined but would include automotive vehicles incorporating ICTS. Despite these regulatory developments, OICTS has until recently remained a nascent office with relatively little enforcement activity. However, that is likely to change in the near term, and companies may soon be faced with a new set of compliance and reporting obligations, along with steep penalties for inaction. On January 29, 2024, Commerce's Bureau of Industry and Security ("BIS") issued a proposed rule aimed at the activities of U.S. IaaS providers, including the training of large AI models. These new rules would require all U.S. IaaS providers and their foreign resellers to establish written Customer Identification Programs ("CIPs") to collect, verify, and maintain identifying information about their foreign customers. Additionally, U.S. IaaS providers would be required to file reports with Commerce whenever they have "knowledge" (defined to cover actual knowledge and an awareness of a high probability, which can be inferred from acts constituting willful blindness) of any transaction between the provider and a foreign person "which results or could result in the training of a large AI model with potential capabilities that could be used

Related People

Adam M. Smith

Stephenie Gosnell Handler

Marcus Curtis

Chris R. Mullen

Christopher T. Timura

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

in malicious cyber-enabled activity."[5] The proposed new rule implements specific provisions of two separate EOs—EO 13,984 issued in the final days of the Trump administration and the aforementioned EO 14,110—and is aimed at addressing threats to U.S. IaaS products and services by foreign malicious cyber actors. Compliances professionals already familiar with Know Your Customer ("KYC") requirements under such existing trade controls regimes as the U.S. Export Administration Regulations ("EAR") administered by BIS and various sanctions programs administered by the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") will recognize much of the language in the proposed compliance requirements. However, the proposed ICTS regulations also contain many unique facets such as customer identification and recordkeeping requirements that require additional consideration. Ultimately, companies that operate in the IaaS and AI fields, as well as related industries, will likely be obliged to implement additional compliance and reporting measures before transacting with certain foreign persons once the proposed regulations come into effect. At present, there is no effective date for the proposed rule, though Commerce has requested public comment on several aspects of the proposed regulations—including whether Commerce should receive and approve all CIPs—by April 29, 2024. Once the comment process concludes, Commerce will then move forward with a "final rule," though additional comments may be requested at Commerce's discretion. However, given the details already included in the proposed rule, a final rule and effective date in the coming months are likely. **Key Terms and Definitions** The definitions in the new regulations clearly articulate the potentially expansive impact the proposed rule is likely to have. For example, the new CIP requirements (discussed in detail below) apply to all U.S. providers of "IaaS products," defined broadly as a product or service offered to a consumer "that provides processing, storage, networks, or other fundamental computing resources, and with which the consumer is able to deploy and run software that is not predefined, including operating systems and applications."[6] A "U.S. IaaS provider" is defined to include any U.S. person that offers any "IaaS product," while the term "U.S. person" is broadly defined to include U.S. citizens and permanent resident aliens, entities organized under U.S. law, and persons present in the United States, similar to the definition of "U.S. person" under EAR.[7] The term "foreign reseller of U.S. [IaaS] products," is similarly broadly defined to include non-U.S. persons who have "established an [IaaS] account to provide [IaaS] products subsequently, in whole or in part, to a third party."[8] Importantly, and as discussed in detail below, such foreign resellers are also subject to certain compliance and reporting requirements under the new regulations. Likely in an attempt to standardize the definition across various government agencies, "AI" is defined by reference to 15 U.S.C. 9401(3), which defines the term as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to (A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action."[9] While the AI reporting requirements are tied specifically to "large AI model[s] with potential capabilities that could be used in malicious cyber-enabled activity," the technical parameters of this term are not yet wholly defined.[10] Rather, Commerce notes that it will publish applicable technical conditions in a forthcoming *Federal Register* notice, though it remains unclear if these parameters will be published as a proposed or final rule. Where the lines defining the types of "AI" caught under the proposed regulations are ultimately drawn will have a significant impact on many industries, and Commerce appears highly interested in receiving additional input and guidance from members of potentially-impacted industries through the public comment process. **Customer Identification Program Requirement: Collect, Identify, Maintain** The proposed CIP requirement consists of three main components: (1) information collection; (2) customer verification; and (3) recordkeeping. These requirements apply to both U.S. IaaS providers and their foreign resellers. ***Customer information***. The proposed rule provides that all U.S. IaaS providers and their foreign resellers must collect, at minimum, the following information from any potential foreign customer prior to opening an account with that customer:

- Name or business name;

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

- Address (for an entity, the principal place of business and the location(s) from which the IaaS product will be used; for an individual, the street address and the location(s) from which the IaaS product will be used);
- Jurisdiction under whose laws the person is organized (for a person other than an individual);
- Name(s) of beneficial owner(s) of an IaaS account in which a foreign person has an interest (if not held by an individual);
- Means and source of payment for the account (including credit number, account number, and customer identifier);
- Email address;
- Telephonic contact information; and
- IP addresses used for access or administration and the date and time of each such access or administrative action.[11]

Customer verification. The proposed rule also requires the CIP to contain procedures for verifying the identity of potential foreign customers through (i) a "documentary verification method," (ii) a "non-documentary verification method," or (iii) in some cases, a combination of both.[12] The CIP must also address situations where the IaaS provider will obtain further information to verify a customer's identity when other documentary and non-documentary methods fail, or when the attempted verification leads the IaaS provider to doubt the true identity of the potential customer.[13] Finally, the proposed rule requires the CIP to include procedures for situations in which the U.S. IaaS provider cannot reasonably ascertain the identity of a potential customer, including procedures describing (i) when the provider should not open an account for the potential customer, (ii) the terms under which a customer may use an account while the provider attempts to verify the customer's identity (such as restricted permission or enhanced monitoring of the account), (iii) when the IaaS provider should close an account after verification attempts have failed, and (iv) other measures for account management or redress for customers whose identification could not be verified or whose information may have been compromised.[14]
Recordkeeping. The proposed recordkeeping requirements are relatively straightforward. Under the proposed rule, the CIP must include procedures for maintaining a record of the identifying information collected by the provider; retain the required record for at least two years after the date the account is closed (or was last accessed); and include methods to ensure the record will not be shared with any third party. With respect to the content of the record, the proposed rule requires the record to include:

- All identifying customer information listed above;
- A copy or description of any document relied on to verify a customer's identity;
- A description of any methods and the results of any measures used to verify the identity of the customer and the account's beneficial owner(s); and
- A description of the resolution of any substantive discrepancy discovered when verifying identifying information.[15]

While trade compliance professionals have deep familiarity with conducting customer due diligence to satisfy long-standing regulatory requirments, the explicit level of detail that CIPs must address extends beyond the KYC requirements currently outlined by OFAC[16] and BIS.[17] As stated above, the proposed CIP rule applies to both U.S. IaaS providers and their foreign resellers. Indeed, under the proposed rule, U.S. providers are responsible for ensuring their foreign resellers maintain compliant CIPs and for furnishing those CIPs to Commerce within 10 days upon request.[18] In addition, U.S. providers must take appropriate action in response to their foreign resellers' non-compliance with the rule. Specifically, the proposed rule provides that a U.S. IaaS provider must, upon receiving evidence that a foreign reseller has failed to maintain a CIP or to undertake good-faith efforts to prevent the use of U.S. IaaS products for malicious cyber-enabled activities, take

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

steps to (1) terminate the foreign reseller account within 30 days absent remediation by the reseller, and (2) if relevant, report the malicious cyber-enabled activity.[19] According to the proposed rule, Commerce anticipates that compliance with any new CIP regulations would be required within one year of the date of publication of a final rule, which as noted above could be published in the upcoming months. In light of these forthcoming requirements, compliance professionals should revisit and revise, as appropriate, the requirements and procedural guidance associated with their customer due diligence programs. **CIP Certification** Commerce proposes to monitor compliance with the CIP requirement in part by requiring U.S. IaaS providers to certify their CIPs (and the CIPs of their foreign resellers) on an annual basis. Under the proposed rule, each U.S. IaaS provider is required to submit a "CIP certification form" that must include, among other items:

- A description of the systems or tools the IaaS provider uses to verify the identity of foreign customers;
- The procedures the IaaS provider uses to require a customer to notify the provider of any changes to the customer's ownership (including the addition or removal of beneficial owners);
- The systems or tools used by the IaaS provider to detect malicious cyber activity;
- The procedures for requiring each foreign reseller to maintain a CIP;
- The 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 activities;
- The name, title, email, and phone number of the primary contact responsible for managing the CIP;
- A description of the IaaS provider's service offerings and customer bases in foreign jurisdictions;
- The number of employees in IaaS provision and related services;
- The process the IaaS provider uses to report any malicious cyber activity;
- The number of IaaS customers;
- The number and locations of the IaaS provider's foreign beneficial owners;
- A list of all foreign resellers of IaaS products; and
- The number of IaaS customer accounts held by foreign customers whose identity has not been verified, including a description and timeline of actions the IaaS provider will take to verify the identity of each customer, among other information.[20]

The annual certification must include various attestations, including attestations that the provider has (i) reviewed its CIP since the date of its last certification; (ii) updated its CIP to account for any changes in its service offerings, the threat landscape, and changes to the applicable regulations since its last certification; (iii) tracked the number of times it was unable to verify the identity of any customer since its last certification; and (iv) recorded the resolution of each situation described in (iii).[21] The proposed rule also requires IaaS providers to notify Commerce outside of the annual reporting cycle in various situations, including when the provider undergoes a significant change in business operations or corporate structure, or if the provider implements a material change to its CIP, such as a material change in its customer verification methods.[22] Importantly, newly established IaaS providers will be required to submit a CIP certification prior to furnishing any foreign customer with an IaaS account.[23] **Compliance Assessments** Commerce plans to use compliance assessments to enforce the proposed CIP requirement. Under the proposed rule, Commerce will, after reviewing CIP certification forms, and "at its sole discretion as to time and manner," conduct compliance assessments of certain U.S. IaaS providers

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

based on the risks associated with a given CIP, U.S. IaaS provider, or any of the provider's foreign resellers.[24] Commerce similarly has the power to request an audit of any U.S. IaaS provider's CIP processes and procedures. The evaluation of potential risks by Commerce will consider, among other criteria, whether the services or products of the U.S. provider or foreign reseller are likely to be used by foreign malicious cyber actors, or by a foreign person to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity.[25] The proposed rule outlines two general actions Commerce may take based on the results of a compliance assessment. First, Commerce may require a U.S. IaaS provider to take remedial measures, including (i) general measures to address any risk of U.S. IaaS products being used in support of malicious cyber activity, and (ii) "special measures"—including prohibitions or conditions on maintaining accounts with certain foreign persons—to counter malicious cyber-enabled activity. Second, Commerce may decide to review a particular transaction or class of transactions of an IaaS provider. Nothing in the proposed rule limits Commerce to recommending (or requiring) only one specific remedial measure, and it is possible Commerce could impose multiple remedial obligations in response to a compliance assessment.[26] **Exemptions from the CIP Requirement** Although the proposed CIP requirement generally applies to all U.S. IaaS providers and their foreign resellers, the proposed rule allows the Secretary to exempt any provider, any specific type of account or lessee, or reseller from the CIP requirement if the party "implements security best practices to otherwise deter abuse of IaaS products."[27] To satisfy this criterion, a party must establish an Abuse of IaaS Products Deterrence Program ("ADP") that is designed to detect, prevent, and mitigate malicious cyber-enabled activities in connection with their accounts. The ADP must include policies and procedures to (i) identify relevant "Red Flags" (that is, activities that indicate possible malicious cyber-enabled activities) for the relevant accounts; (ii) detect those Red Flags, including by implementing privacy-preserving data sharing and analytics methods as feasible; and (iii) respond appropriately to any Red Flags detected.[28] The ADP (including the relevant Red Flags) must also be updated regularly to reflect changes in risks and must be continuously administered by the U.S. IaaS provider. Establishing an ADP is a necessary, but not sufficient, condition to obtain an exemption from the CIP requirement. Specifically, the proposed rule explains that the Secretary will decide whether to grant an exemption by considering:

- Whether the size and complexity of the ADP is commensurate with the nature of the provider's product offerings;
- Whether the ADP's ability to detect and respond to Red Flags is sufficiently robust;
- Whether oversight of reseller arrangements is effective;
- The extent to which the provider cooperates with law enforcement to provide forensic information for investigations of identified malicious cyber-enabled activities; and
- Whether the provider participates in public-private collaborative efforts, such as consortia to develop improved methods to detect and mitigate cyber-enabled activities.[29]

Even after an ADP is deemed sufficient by the Secretary, the proposed regulations are clear that the exemption may be revoked at any time, including to impose special measures as described below. **Special Measures** The overarching purpose of the CIP requirement is to prevent foreign persons from using U.S. IaaS products to conduct malicious cyber-enabled activities. Consistent with that purpose, the proposed rule permits the Secretary to require providers to take "special measures" if the Secretary determines that "reasonable grounds exist for concluding that a foreign jurisdiction or foreign person is conducting malicious cyber-enabled activities using U.S. IaaS products."[30] These "special measures" include (1) prohibitions or conditions on opening or maintaining accounts within a foreign jurisdiction that has a significant number of foreign persons offering or obtaining U.S. IaaS products used for malicious cyber activity; and (2) prohibitions or conditions on maintaining an account with a foreign person who has a

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

pattern of conduct of obtaining or offering U.S. IaaS products for use in malicious cyber activities.[31] In selecting which special measure to take, the Secretary will consider:

- Whether the imposition of any special measure would create a "significant competitive disadvantage" for U.S. IaaS providers, including due to any undue burden associated with compliance;
- The extent to which the timing of any special measure would have a "significant adverse effect on legitimate business activities" involving the particular foreign jurisdiction or foreign person; and
- The effect of any special measure on U.S. national security or foreign policy, law enforcement investigations, U.S. supply chains, or public health.[32]

Any special measure imposed under the proposed rule may not remain in effect for more than 365 calendar days (absent publication of a notice of extension), and a U.S. IaaS provider has 180 days following the Secretary's determination that a special measure is required before it must implement the measure.[33] **Reporting of Large AI Model Training** The second key piece of the proposed rule requires U.S. IaaS providers to submit a report to Commerce whenever they have "knowledge" (as defined above) of any transaction between the provider and 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."[34] The proposed rule defines "large AI model" as any AI model with the technical conditions of a "dual-use foundation model" or that "otherwise has technical parameters of concern" that enable the AI model to "aid or automate aspects of malicious cyber-enabled activity," though as noted previously, the technical parameters defining what exactly constitutes a large AI model are forthcoming.[35] For covered transactions involving such AI models, the proposed rule requires U.S. IaaS providers to report to Commerce, within 15 calendar days of a covered transaction occurring (or the provider or reseller having knowledge that a covered transaction has occurred) (i) certain identifying information about the foreign customer (such as name, address, means and source of payment, and the location from which the training request originates) and (ii) information about the training run itself, including the estimated number of computational operations used in the training run, the model of the primary AI used in the training run accelerators, and information on cybersecurity practices, among others.[36] U.S. IaaS providers must also require their foreign resellers to submit similar reports to the provider within 15 calendar days whenever the reseller has knowledge of a covered transaction, after which the provider must file the report with Commerce within 30 calendar days of the covered transaction.[37] Following such reports, Commerce may initiate follow-up requests to which the U.S. IaaS provider must respond within 15 calendar days.[38] Finally, under the proposed rule, no U.S. IaaS provider may provide IaaS products to a foreign reseller unless the provider has made all reasonable efforts to ensure the reseller has complied with the large AI model training reporting requirement.[39] **Penalties and Enforcement** Even though related ICTS regulations already permit penalties, Commerce has proposed new enforcement provisions specifically tied to non-compliance with the proposed rule. Violations can result in civil monetary fines of up to $364,992 per violation (an amount adjusted annually for inflation) or twice the value of the transaction, whichever is greater. Criminal penalties involving fines up to $1,000,000, imprisonment for up to 20 years, or both are also available in cases involving willful violations.[40] Under the proposed rule, violations would include the following:

- Engaging in, or conspiring to engage in, any conduct prohibited by the proposed regulations;
- Failing to submit reports, certifications, or recertifications, as appropriate, or failing to comply with terms of notices or orders from Commerce;
- Failing to implement or maintain CIPs as required, or continuing to transact with a foreign reseller that fails to implement or maintain a CIP as set forth in the regulations;

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

- Providing IaaS products to a foreign person while failing to comply with any direction, determination, or condition issued under the regulations;
- Aiding, abetting, counseling, commanding, inducing, procuring, permitting, approving, or otherwise supporting any act prohibited by any direction, determination, or condition issued under the regulations;
- Attempting or soliciting a violation of any direction, determination, or condition issued under the regulations;
- Failing to implement any required prohibition or suspension related to large AI model training; and
- Making a false or misleading representation, statement, notification, or certification, whether directly or indirectly through any other person, or falsifying or concealing any material fact to Commerce related to compliance with the regulations.[41]

Looking Forward The proposed rule has significant implications for U.S. IaaS providers and their resellers, requiring the implementation of robust CIPs, certification of those programs on an annual basis, and, under some circumstances, the imposition of "special measures" against a foreign jurisdiction or foreign person when that jurisdiction or person obtains products for use in malicious cyber activities. As discussed previously, the proposed rule also requires IaaS providers and their foreign resellers to report transactions with foreign persons that involve training large AI models with potential capabilities for malicious cyber-enabled activity. Although a final rule is likely still several months away, IaaS providers can take several steps now to prepare for the new regulations and ease the transition to the new reporting regime:

- **Provide Written Comments**: Commerce is soliciting public comment on various aspects of the proposed rule, including on whether it should receive and approve all CIPs, and whether there currently exist best practices for customer identification and verification that IaaS providers can use as a model for their CIPs. Companies must provide comments by email (IaaScomments@bis.doc.gov) or at regulations.gov by April 29, 2024.

- **Review and Enhance Current Practices**: IaaS providers can perform an internal review of their current customer identification and verification practices to assess how those practices align with the proposed CIP requirements and identify areas that fall short of those requirements. Such a review would allow providers to jumpstart their compliance efforts and prepare for any required reports.

- **Take Stock of Foreign Resellers and Foreign Customers**: Because the reporting obligations apply to U.S. IaaS providers ***and*** their foreign resellers, providers may find it beneficial to evaluate their existing reseller relationships and the extent to which their resellers take steps to verify the identity of their customers and operate using cybersecurity best practices. U.S. IaaS providers may also consider reviewing the compliance obligations in their contracts with foreign resellers to ensure that the requirements under the proposed rule are sufficiently covered.

- **Identify AI Training-Related Accounts**: IaaS providers should review current and potential future accounts that may fall within the proposed rule's definition of transactions involving "large AI model training." The turnaround time for reporting such transactions is relatively short (15 calendar days), so providers may be well-served by conducting a preliminary assessment of their obligations under this part of the proposed rule before the final rule goes into effect. Providers may also wish to proactively develop or enhance procedures for responding to instances of suspected training of large AI models for use in malicious cyber-enabled activities to ensure all appropriate deadlines are met.

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Gibson Dunn attorneys remain ready to assist companies with these preparatory steps or to address any questions about the potential role that OICTS may play in the near future.

_____ [1] Exec. Order No. 13,873, 84 Fed. Reg. 22,689 (May 17, 2019). [2] Exec. Order No. 13,984, 86 Fed. Reg. 6,837 (Jan. 25, 2021). [3] Exec. Order No. 14,034, 86 Fed. Reg. 31,423 (June 11, 2021). [4] Exec. Order No. 14,110, 88 Fed. Reg. 75,191 (Nov. 1, 2023). [5] Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities, 89 Fed. Reg. 5,698, 5,733 (Jan. 29, 2024) [hereinafter NPRM]. [6] *Id*. at 5,726. [7] *Id*. at 5,727. [8] *Id*. at 5,726. [9] 15 U.S.C. 9401(3). [10] NPRM, *supra* note 5, at 5,727. [11] *Id*. at 5,727-28. [12] *Id*. at 5,728. [13] *Id*. [14] *Id*. [15] *Id*. [16] *See* OFAC, A Framework for OFAC Compliance Commitments 4 (May 2, 2019), https://ofac.treasury.gov/media/16331/download?inline. [17] *See* 15 C.F.R. Part 732, Supplement No. 3. [18] NPRM, *supra* note 5, at 5,729-30. [19] *Id*. at 5,729. [20] *Id.* [21] *Id*. [22] *Id*. [23] *Id*. at 5,730. [24] *Id*. [25] *Id*. [26] *Id.* [27] *Id.* [28] *Id.* at 5,730-31. [29] *Id*. at 5,731-32. [30] *Id*. at 5,732. [31] *Id.* [32] *Id*. at 5,733. [33] *Id*. at 5,732. [34] *Id*. at 5,733 (emphasis added). [35] *Id*. at 5,727. [36] *Id*. at 5,734. [37] *Id*. [38] *Id*. [39] *Id*. [40] *Id*. at 5,735. [41] *Id*. at 5,734.

The following Gibson Dunn lawyers prepared this update: Adam Smith, Stephenie Gosnell Handler, Chris Timura, Marcus Curtis, and Chris Mullen.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these issues. For additional information about how we may assist you, please contact the Gibson Dunn lawyer with whom you usually work, the authors, or the following leaders and members of the firm's International Trade or Privacy, Cybersecurity & Data Innovation practice groups: **International Trade**: Adam M. Smith – Washington, D.C. (+1 202.887.3547, asmith@gibsondunn.com) Stephenie Gosnell Handler – Washington, D.C. (+1 202.955.8510, shandler@gibsondunn.com) Christopher T. Timura – Washington, D.C. (+1 202.887.3690, ctimura@gibsondunn.com) David P. Burns – Washington, D.C. (+1 202.887.3786, dburns@gibsondunn.com) Marcus Curtis – Orange County (+1 949.451.3985, mcurtis@gibsondunn.com) Chris R. Mullen – Washington, D.C. (+1 202.955.8250, cmullen@gibsondunn.com) Samantha Sewall – Washington, D.C. (+1 202.887.3509, ssewall@gibsondunn.com) **Privacy, Cybersecurity and Data Innovation**: S. Ashlie Beringer – Palo Alto (+1 650.849.5327, aberinger@gibsondunn.com) Jane C. Horvath – Washington, D.C. (+1 202.955.8505, jhorvath@gibsondunn.com) Vivek Mohan – Palo Alto (+1 650.849.5345, vmohan@gibsondunn.com) © 2024 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

Related Capabilities

International Trade Advisory and Enforcement

Privacy, Cybersecurity, and Data Innovation

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**