wiley

ALERT

A Final Trump EO Would Regulate Cloud, Software and Remote Computing Services

January 21, 2021

On January 19, 2021, President Trump issued an *Executive Order on Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities* (EO), designed to regulate United States Infrastructure as a Service (IaaS) products, in order to address concerns about use by foreign malicious actors. This EO was part of a flurry of national security actions by the outgoing Administration related to technology. If implemented, this EO would impose "know your customer" (KYC) type requirements on many technology companies and could expand government's ability to monitor and track users of various internet and IT services.

Given the EO's potentially broad impact, industry should monitor the Biden Administration's treatment of the EO and any rules that the Commerce Department may draft as required under the EO. Notably, on January 20th, the new Administration announced a temporary pause on regulatory actions to allow incoming officials the opportunity to review and approve pending agency actions. This analysis identifies key provisions and obligations in the EO, areas of uncertainty for U.S. companies, and possible next steps as the Biden Administration assumes control over key agencies.

What does this EO Do?

The stated purpose of the EO is "to deal with the national emergency related to significant malicious cyber-enabled activities" by foreign nationals. Specifically, the EO aims to deter foreign adversaries from using IaaS services, like virtual private networks (VPNs), that can allow for anonymous activity on the Internet, by requiring IaaS providers to verify and document the identity of foreign nationals that use these services. Ideally, the EO seeks to make it harder for foreign

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Privacy, Cyber & Data Governance
White Collar Defense & Government Investigations

adversaries to engage in cyber-attacks anonymously and help United States law enforcement track the sources of attacks.

However, the EO and contemplated regulations could have dramatic, sweeping impacts on legitimate Internet use far beyond the targeted foreign adversaries. The contemplated regulations could alter how many Internet services are offered, impacting not just the companies that provide these services, but consumers, corporations, and entities that rely on them.

The EO calls for three main actions:

- New regulations that require IaaS providers to take steps to identify foreign nationals that use their services;
- New regulations that allow the Commerce Department to prohibit or impose conditions on any IaaS accounts that are operated by a foreign national that are involved in malicious cyber-enabled activities; and
- A report by Commerce, the U.S. Department of Homeland Security (DHS), and the U.S. Department of Justice (DOJ) with recommendations to increase threat sharing between IaaS providers and the United States about malicious cyber activity.

What is IaaS?

The EO casts a wide net. IaaS Products are defined as:

> "**[A]ny product or service** offered to a consumer, including complimentary or 'trial' offerings, 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...The term is inclusive of 'managed' products or services, in which the provider is responsible for some aspects of system configuration or maintenance, and 'unmanaged' products or services, in which the provider is only responsible for ensuring that the product is available to the consumer..." (emphasis added).

This is potentially sweeping. Depending on how the U.S. Department of Commerce frames proposed regulations, the definition could reach providers of cloud services, remote computing services, network management platforms, and possibly some social media applications. As drafted, the EO does not seem to distinguish between SaaS or other cloud services, and IaaS and could include services like cloud-based email, storage, messaging or other social media services. Until implementing regulations more clearly define the intended scope of covered IaaS, the EO's impact is unclear. If interpreted broadly, it has the potential for enormous reach.

Covered Providers Would have to Verify Users' Identity

The EO directs the Secretary of Commerce to propose regulations within 180 days that would require IaaS providers to take steps to identify foreign nationals that open or maintain accounts for IaaS services. These steps include keeping records on the name, national identification number, address, means and source of payment, email and telephone number, and IP addresses used to access the account. Similar to "know your customer" requirements under other legal authorities, the EO is aimed at imposing:

> "[R]ecord-keeping obligations with respect to foreign transactions. To address these threats, to deter foreign malicious cyber actors' use of United States IaaS products, and to assist in the investigation of transactions involving foreign malicious cyber actors, the United States must ensure that providers offering United States IaaS products verify the identity of persons obtaining an IaaS account ('Account') for the provision of these products and maintain records of those transactions."

The United States has often considered expanding the Communications Assistance for Law Enforcement Act (CALEA), which requires covered communications providers to have the capability to implement wiretaps. The "record keeping obligations" of the new regulations, depending on how drafted, could become the equivalent of CALEA-type requirements for Internet services.

The Government Would Prohibit Certain IaaS Accounts

The EO directs the creation of regulations that would allow the government to prohibit IaaS providers from offering services to certain end user accounts associated with foreign malicious cyber-attacks. Within 180 days, the Secretary of Commerce shall propose regulations, with an opportunity to comment, that require United States IaaS providers to prohibit or impose conditions on the opening or maintaining in the United States an Account, including a Reseller Account, for or on behalf of (1) any foreign person located in certain foreign jurisdictions or (2) certain foreign persons.

The Government Can Identify Foreign Jurisdictions or Persons Responsible for Malicious Cyber Activity. The EO enables the government to target certain countries and foreign persons known for using or reselling the IaaS of U.S. companies used for malicious cyber activity.

- ***Identifying Jurisdictions:*** The Secretary is to consult with heads of other agencies to determine if "a foreign jurisdiction has any significant number of foreign persons offering United States IaaS products that are used for malicious cyber-enabled activities or any significant number of foreign persons directly obtaining United States IaaS products for use in malicious cyber-enabled activities." To determine if jurisdictions are covered, factors include the extent to which that foreign jurisdiction is a source of malicious cyber-enabled activities and whether there is a mutual legal assistance treaty (MLAT) with that jurisdiction, among others.
- ***Identifying Individuals:*** Similarly, a determination shall be made related to certain foreign persons. Several factors shall be considered, including the extent of that individual's use of United States IaaS to promote malicious cyber-enabled activities. The creation of lists of foreign jurisdictions and persons that will be effectively prohibited from the use of covered IaaS services mirrors existing sanctions efforts, like OFAC sanctions lists maintained by the U.S. Department of Treasury. Curiously, the EO does not

reference other U.S. sanctions regimes, suggested the new regulations may take a broader approach.

The EO Authorizes Government to Adopt Special Measures and Prohibitions. The EO permits the Secretary to "prohibit or impose conditions on the opening or maintaining with any United States IaaS provider of an Account, including a Reseller Account," by any foreign person located in a foreign jurisdiction or certain foreign persons. This could be broadly interpreted to invite government scrutiny and special regulations of companies' operations and account management practices.

In determining what special measures shall be imposed, the Secretary must consider: (i) if "any special measure would create a significant competitive disadvantage, including any undue cost or burden associated with compliance, for United States IaaS providers; (ii) the extent to which the imposition of any special measure or the timing of the special measure would have a significant adverse effect on legitimate business activities involving the particular foreign jurisdiction or foreign person; and (iii) the effect of any special measure on United States national security, law enforcement investigations, or foreign policy."

The Government Wants to Expand Information Sharing by and with IaaS Providers

Within 120 days of the EO, the Attorney General and Secretary of DHS, in coordination with the heads of Commerce and other agencies, shall solicit feedback from industry "on how to increase information sharing and collaboration among IaaS providers" with the federal government. A report shall be drafted to encourage the "(i) voluntary information sharing and collaboration, among United States IaaS providers; and (ii) information sharing between United States IaaS providers and appropriate agencies, including the reporting of incidents, crimes, and other threats to national security[.]" Among other things, the report shall include recommendations for liability protections beyond those in existing law that may be needed to encourage greater information sharing in this context.

Looking Ahead, the Tech Sector Should Expect Scrutiny

The EO and any implementing regulations could have a far-reaching impact on providers of cloud services and other ICT and data management services. As the Biden Administration begins, it is unclear the extent to which the EO will remain in force or be implemented by Commerce Department rules. If rules are developed, the private sector should consider how to encourage a narrow scope and a more pragmatic approach to security concerns.

Big picture, concerns about foreign adversary use of domestic technology platforms and services are likely to remain, particularly in law enforcement and intelligence agencies that have been uneasy about "no log" VPNs or "bulletproof hosting." Federal authorities last month took action to shut down some such services, and have expressed concern about obfuscated identifies and activities online. Because cyber incidents and vulnerabilities from malicious foreign actors continue to impact national security and the economy, it is likely that there will be at least some appetite among officials in the new Administration to engage with industry on identifying users of technology and services in the United States.