ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

700 K Street NW Suite 600
Washington, DC 20001

COMMENTS OF ITIF

Before the

Bureau of Industry and Security, Department of Commerce,

Washington, D.C.

In the Matter of:	)	
Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities	)	MB Docket No. 240119-0020

April 29, 2024

TABLE OF CONTENTS

Introduction and Summary 2

The Biden Administration Needs to Provide More Public Evidence About the Specific Nature of IaaS-Based Cybersecurity Threats 3

Change the Exemptions Framework: Provide Clear and Broad Exemptions for Good Cybersecurity Firms, And Target Bad Ones for Additional Action 4

Know-Your-Customer Reporting, Identity Verification, and Suspicious Activity Reports for Cloud Services are Likely to be Problematic and Ineffective 5

IAAS Customer Reporting Requirements Raise Domestic and International Privacy Concerns 6

Forcing U.S. IaaS Firms to Report on Foreign AI Use is Highly Problematic 7

IAAS AI and KYC Reporting Requirements will Impact U.S. Competitiveness and Trade 8

At a Minimum, Create a Review Mechanism and Criteria to Assess Program Effectiveness 8

Focus on, and Fix, Public-private Information Sharing and Collaboration 9

Address Cloud-related Issues as Part of International Collaboration and Information Sharing on Cybersecurity 10

Conclusion 11

INTRODUCTION AND SUMMARY

The Information Technology and Innovation Foundation (ITIF) welcomes the opportunity to submit comments in response to the advance notice of proposed rulemaking (ANPRM) on "Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities."[1] ITIF is a non-profit, non-partisan public policy think tank focused on technological innovation and public policy.

ITIF agrees with the goal of the executive order—to ensure that foreign actors do not exploit U.S. cloud computing resources for malicious cyber activities—but the proposed solutions have multiple deficiencies which would not only render them ineffective, but also undermine the competitiveness of U.S. cloud computing providers. Creating and sharing customer information would create new data privacy risks for customers of U.S. cloud providers, as they would be required to provide sensitive personal and business information in an unsecured format (e.g., scans of paper identity documents). It's also unclear whether this information would be useful in combating malicious cyber activity (as actionable information is context specific in terms of responding to cyber threats and attacks). In addition, hackers may specifically target U.S. IaaS cloud service providers to illegally obtain these identity-proofing documents.

Cyberattackers (whether nation-state-backed or cybercriminals) abuse a diverse range of U.S. and global IT services in a constantly varying range of ways to conduct attacks. Malicious actors consistently route their attacks via intermediaries to avoid cyber threat detection and defenses. Like U.S. Infrastructure as a Service

(IaaS) providers, intermediary services like virtual private servers, remote storage, and domain hosting are often similarly misused or abused by cyberattackers. Malicious actors can acquire virtual resources either legitimately (e.g., as a customer), fraudulently (e.g., using stolen credit cards or stolen identities), or surreptitiously (e.g., compromise of legitimate customer accounts). All providers face a similar challenge to differentiate between malicious actors and legitimate users. It's difficult for any one actor to single-handedly detect and respond to malicious actors.

Perhaps most important to this proposal is the point that the intended goal of the proposal is to identify and stop unlawful foreign customers, and these bad actors are not going to play by the rules. They will lie and cheat to gain access to U.S. IaaS services, such as by using stolen payment credentials, masquerading their identity, hiding behind a network of shell companies, or buying access to verified IaaS accounts in the underground economy. Therefore, any identity verification requirements should be designed with the assumption that those bad actors the government most wants to find will be the ones most likely to attempt to circumvent and adapt to the requirements.

Instead, as the National Security Telecommunications Advisory Committee (NSTAC)'s report on the abuse of domestic infrastructure (ADI) recommends, the U.S. government should create a holistic strategy to combat the abuse of ADI as "no singular action or approach will fully address the challenge on its own" and that this should not focus on foreign actors but overall abuse no matter where the threat actor is located as "there is no technical or other consistent method that can be employed to distinguish ADI between foreign actors and domestic actors with speed and accuracy at the macro level, especially for routine online business transactions."[2] The United States should work with likeminded countries to remove legal barriers and uncertainty to ensure that cloud and other IT firms have clear legal frameworks and mechanisms to share information with government authorities to better detect and respond to malicious cyber activity.

If the United States pushes ahead with this IaaS reporting requirement, law-abiding foreign customers might simply opt to go with an alternative non-U.S. cloud provider to avoid the risk. At a time when U.S. cloud providers are seeking to compete in foreign markets, this proposal could undermine trust in U.S. cloud providers by creating the appearance, if not the reality, of potentially inappropriate interference by the U.S. government of foreign users of domestic IaaS cloud service providers.

THE BIDEN ADMINISTRATION NEEDS TO PROVIDE MORE PUBLIC EVIDENCE ABOUT THE SPECIFIC NATURE OF IAAS-BASED CYBERSECURITY THREATS

The Biden administration has not presented a clear body of evidence to justify why this (as opposed to other policy options) proposal is needed and how exactly it would be effective to address the malicious use of U.S. IaaS. In 2015, the United States first declared a national emergency with respect to significant malicious cyber-enabled activities.[3] This was recently renewed in March 2024.[4] Yet, nearly a decade into this national emergency, there's still little public information about the exact nature of the threat and how this proposed IaaS regime would complement other efforts to counter this malicious cyber activity. The ANPRM simply states that "foreign malicious cyber actors have utilized U.S. IaaS products to commit intellectual property and sensitive data theft, to engage in covert espionage activities, and to threaten national security by targeting U.S. critical infrastructure."

Given the lack of detailed evidence, it's unclear whether the cost and complexity of creating this system is worth it from a cost-benefit perspective. As it stands, the overwhelming conclusion is that the proposed IaaS regime would not be effective in preventing IaaS-based malicious cyber activities.[5] If the Biden administration provided more data and evidence to inform the debate, U.S. stakeholders would be more willing to support the proposed IaaS regime given the significant costs and complexities involved. As it stands, the trade-off does not make sense. Not only that, but there's the real risk that this IaaS regime actually detracts from cloud's role in cybersecurity as it diverts resources and attention away from actions that actually identify and address malicious cyber activities.

This proposed IaaS regime appears disconnected from other U.S. government initiatives to respond to malicious cyber activity, such as Chinese-state sponsored cyber actors (known as Volt Typhoon) seeking to pre-position themselves on information technology (IT) networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States.[6] It's unclear whether the proposed IaaS regime would stop a sophisticated and persistent threat actor like Volt Typhoon, which used valid accounts and leveraged strong operational security, which combined, allowed for a long-term undiscovered persistence. Volt Typhoon actors maintained access and footholds within some victim IT environments for at least five years. Volt Typhoon actors conduct extensive pre-exploitation reconnaissance to learn about the target organization and its environment; tailor their tactics, techniques, and procedures to the victim's environment; and dedicate ongoing resources to maintaining persistence and understanding the target environment over time, even after initial compromise.[7]

While it is important for national security to prevent foreign adversaries from leveraging U.S. IaaS for malicious purposes and geostrategic advantage, it is also critical for U.S. economic security and technology leadership not to undermine the critical role that cloud plays in modern commerce. So, before enacting laws and regulations that will redefine the U.S. approach to cloud and data governance, the Biden administration should disclose detailed information regarding how this regime would stop Chinese and other malicious actors from engaging in cyberattacks. The Biden administration needs to do a better job of presenting evidence about the risk (and practices) of Chinese and other malicious actors to better inform the debate. More transparency would not only help inform debate in the United States, but it would also help get the United States to work with likeminded countries on how they can work together to combat malicious cyber activity.

The Biden administration's motivation to do something to address a legitimate issue (such as Chinese cyber threats) should not mean it commits to a regime that is based on limited data/evidence of uncertain effectiveness. The Biden administration should not let the motivation to do something overpower careful considering of a proposal that has clear deficiencies.

CHANGE THE EXEMPTIONS FRAMEWORK: PROVIDE CLEAR AND BROAD EXEMPTIONS FOR GOOD CYBERSECURITY FIRMS, AND TARGET BAD ONES FOR ADDITIONAL ACTION

The proposed IaaS regime's structure is the reverse of what it should be in providing a clear and broad exemption for U.S. IaaS firms that are clearly committed to addressing cybersecurity threats and additional responsibilities for those firms that are not doing enough or are not doing the right things to address malicious cyber activity.

The proposed IaaS regime does not provide clear and direct assurances that if a firm satisfies the criteria for an exemption, that it'll get an exemption for a significant period. The exemption could arbitrarily be given and taken away. More importantly, the Biden administration should focus on cloud (and other tech firms) that are not cooperating with the U.S. government and are not committed to good cybersecurity practices and setting out additional reporting and other requirements. The proposed IaaS regime mixes up its use of incentives and disincentives (in terms of exempting firms requiring them to take additional action) for the type of action and behavior it expects from U.S. IaaS providers. It fails to differentiate and reward/punish U.S. IaaS firms regardless of whether they're committed to best-in-class cybersecurity measures and public-private cybersecurity cooperation.

The U.S. government's focus should be on how U.S. cloud firms can better coordinate and work with the U.S. government to identify and respond to malicious cyber activities and how to build this out as a central pillar of U.S. efforts is to effectively address this complex issue. If there are IaaS firms that aren't doing enough to address malicious cyber activities or aren't doing the right things, then the U.S. government should set out additional responsibilities for them (i.e., the disincentive).

KNOW-YOUR-CUSTOMER (KYC) REPORTING, IDENTITY VERIFICATION, AND SUSPICIOUS ACTIVITY REPORTS FOR CLOUD SERVICES ARE LIKELY TO BE PROBLEMATIC AND INEFFECTIVE

The Biden administration's proposed know-your-customer (KYC) requirement for U.S. IaaS providers is highly problematic. The KYC requirement requires U.S. IaaS providers to verify the identity of foreign users of U.S. IaaS products, to issue standards and procedures that the Department of Commerce may use to make a finding to exempt IaaS providers from such a requirement, to impose recordkeeping obligations with respect to foreign users of U.S. IaaS products, and to limit certain foreign actors' access to U.S. IaaS products in appropriate circumstances. This includes foreign persons acting as a lessee or sub-lessee of these products or services.[8]

While the draft proposal suggests that identity verification requirements would only apply to foreign customers (not U.S. customers), cloud service providers cannot easily distinguish between domestic and foreign customers. Indeed, there is no way to effectively distinguish between foreign and domestic customers without requiring domestic customers to also prove their identity to show that they are not a foreign customer (otherwise it would be trivial for a foreign customer to avoid these requirements by asserting that they are a domestic customer).

Effectively verifying the identity of customers is not a trivial exercise. In the absence of widely available electronic identification (eIDs), identity verification constitutes a manual process. As a result, cloud service providers would be tasked with manually verifying identity documents or proof of business registration in multiple languages from countries around the world—all remotely. Most cloud service providers are not equipped to handle this task or complete it effectively to prevent fraud. Therefore, imposing this type of requirement could add substantial delays to onboarding new customers which could make U.S. cloud service providers less attractive to foreign customers.

The KYC requirement was proposed, in part, to increase the availability of records that could be useful for investigations into malicious cyber activity. However, there are significant concerns about whether the type of information IaaS providers are supposed to provide as part of the KYC requirement would actually be useful

for combating malicious cyber activity (especially given the lack of public evidence about the specific nature of the threat), especially in comparison to other efforts to improve public-private information sharing that don't involve such a broad and unclear regime as in this proposed KYC framework. Given the broad and diverse nature of cybersecurity threats, the value of information shared depends on its context. U.S. government representatives have noted that relevant information is "situation-specific and circumstantial, and there is no one answer all of the time."[9]

U.S. government officials referred to the U.S. financial sector (under the U.S. Bank Secrecy Act) suspicious activity reports (SARs) as a model for the U.S. IaaS KYC and reporting regime.[10] Many of the same concerns about the role and value of a KYC requirement apply to the potential idea for suspicious activity reports (SARs) for cyber activity, akin to SARs that financial institutions must file with the Financial Crimes Enforcement Network under the Bank Secrecy Act (to detect money laundering or fraud). U.S. financial institutions have to file SARs with the Financial Crimes Enforcement Network whenever there is a suspected case of money laundering or fraud, such as cash transactions over $10,000 per day. However, this seems a bad, or at least incomplete, model for IaaS. Financial institutions see the content of financial transactions, which makes their reports much more useful, while U.S. IaaS firms generally do not have access to their customer's content. It's also unclear whether the information provided under cybersecurity-focused SARs would actually be useful to identify and respond to malicious cyber activity as this is of a very different nature to financial transactions. For example, information shared for the purposes of disruption, mitigation, or future prosecution may not be the same information shared for the purpose of supporting the U.S. government's ability to understand the exact nature of malicious cyber activity, which would be used to develop better indicators to identify future malicious activity. Furthermore, information shared as part of SAR is one way: from U.S. financial firms to the government. In the cybersecurity context, this information sharing is two-way, and ideally, continuous and context specific.

It's also harder to create meaningful thresholds in the context of cloud services in terms of determining what activity would act as a threshold for a SAR and how this information would be useful for preventing and responding to malicious cyber activity. It's also unclear who within the U.S. government would play the equivalent role as U.S. financial regulators and whether they have the resources and expertise to receive, analyze, and respond to information that U.S. IaaS organizations would provide. The financial sector analogy also implies that U.S. IaaS providers would have to create comparable regulatory compliance capabilities, which would be significant. The Bank Secrecy Act also includes a safe harbor for financial institutions that does not apply to U.S. IaaS providers. For example, while the Cybersecurity Information Sharing Act of 2015 encourages the sharing of a circumscribed set of cyber threat information, U.S. firms remain uncertain about the legal risk of participating in some threat intelligence exchanges.[11]

IAAS CUSTOMER REPORTING REQUIREMENTS RAISE DOMESTIC AND INTERNATIONAL PRIVACY CONCERNS

Gathering and sharing identity and activity documents and information would create potential new domestic and international data privacy risks for customers of U.S. cloud providers, as they would be required to provide sensitive personal and business information in an unsecured format (e.g., scans of paper identity documents).

The proactive KYC reporting requirement raises concerns about compliance with the U.S. Electronic Communications Privacy Act of 1986 (ECPA) given it involves customer names and addresses and other records held by U.S. IaaS firms. ECPA prohibits U.S. firms from disclosing this information unless one of ECPA's exceptions applies, such as for law enforcement access, user consent, and government use of warrants and administrative subpoenas.[12] It does not appear that this IaaS reporting requirement would qualify as one of these exemptions.

Many countries (and states/provinces) have data privacy laws that constrain how firms collect, process, store, transfer, and disclose their customer's personal information. These laws and regulations typically apply to information used to identify a specific person (e.g., name, address, date of birth, etc.), but may also apply to infrastructure-related identifiers, such as email addresses and IP addresses. KYC and SAR reporting requirements would only heighten these privacy concerns in foreign jurisdictions. The collection and reporting of personal data to the U.S. government would likely become another point of conflict with trading partners like the European Union. While the Biden administration has engaged trading partners in Asia, Europe, and elsewhere on its proposed data security executive order, and these countries have actively followed developments, there has been a lack of attention paid to the privacy implications of this IaaS regime, but inevitably, they will come, as it bears too many similarities to other policies that have created privacy issues, such as the Transatlantic Data Privacy Framework and the U.S. CLOUD Act.

The European Union would inevitably act against the U.S. IaaS's proposed KYC requirement. In the aftermath of the Court of Justice of the European Union's decision in the "Schrems II" case invalidating the U.S.-EU Privacy Shield, European Union data protection authorities are scrutinizing the ability of U.S. cloud firms to process the personal data of EU citizens given concerns about the U.S. government's ability to access such data. France and other EU member countries already use the hypothetical threat of extraterritorial U.S. government access under the CLOUD Act to justify a range of laws and regulations that specifically target U.S. tech firms and products. For example, France's cloud cybersecurity and labeling regime (known as SecNumCloud) includes discriminatory and restrictive provisions that effectively preclude U.S. and foreign cloud firms as being deemed "trusted" due to concerns about the fear of the U.S. CLOUD Act's potential extraterritorial reach (although this issue is not explicitly mentioned anywhere in the proposal).[13] France has a track record of disregarding cooperation and constructive alternatives to address concerns over government access to data, including the use of technical measures and ongoing bilateral and G7 discussions and negotiations over law enforcement and government access to data.[14] It's easy to see how France could use the IaaS reporting regime in a similar way.

FORCING U.S. IAAS FIRMS TO REPORT ON FOREIGN AI USE IS HIGHLY PROBLEMATIC

The U.S. government proactively obtaining information about foreign customers' use of U.S. IaaS services above a certain compute threshold is highly problematic. There's the potential for the IaaS regime's reporting requirements on AI to essentially become the CLOUD Act of AI reporting in that it forces IaaS firms to report to the U.S. government about their customers' use of services for AI development. Just as the U.S. government's potential use the CLOUD Act to extraterritorially access data held by U.S. firms overseas promoted countries to enact laws and regulations to disadvantage U.S. firms, so too could this IaaS regime impact U.S. IaaS firms and their ability to compete for customers that want to engage them to develop AI.

Executive Order 14110, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," calls for the Department to require U.S. IaaS providers to ensure that their foreign resellers verify the identity of foreign users and provides the Department with authority to require U.S. IaaS providers to submit a report to the Department whenever a foreign person transacts with them to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity. This report, at a minimum, must include the identity of the foreign person and the existence of a training run that meets the criteria set forth in this section, as well as any other information specified in regulation.

Foreign users (whether they are government, private sector, academia, or otherwise) do not want the U.S. government to know why and how they're using cloud services. Their use could involve confidential and trade secret-protected information that U.S. IaaS cloud users don't want IaaS companies sharing. Users also don't want U.S. IaaS firms monitoring and reporting on their cybersecurity practices in terms of how they use their IaaS services.

U.S. IaaS firms do not collect this type of specific usage information about their customers, in part, as it's none of their business in how customers use their services for legitimate business purposes. IaaS firms don't want to become intermediaries that monitor and report on their usage. IaaS firms offer various technical and administrative controls explicitly to help protect users and their use of their services, such as ensuring access controls so only they have access to their AI model and training data.

The requirement is also problematic as the compute threshold (which has not been clearly defined and specified) involves the assumption that users that breach this threshold are somehow involved in malicious activity and AI development that should be of concern to the U.S. government. It also fails to recognize that such arbitrary thresholds don't mean much when AI capabilities continue to change and that malicious actors can game the threshold in operating just below it.

IAAS AI AND KYC REPORTING REQUIREMENTS WILL IMPACT U.S. COMPETITIVENESS AND TRADE

The broad, and potentially intrusive, authority in this proposed IaaS regime will make it harder for U.S. cloud service providers to compete in foreign markets. Foreign customers often express reservations about potential U.S. government access to their systems and data, and this new authority would only exacerbate their concerns. In particular, given the sensitive dialogues between the United States and the European Union over implementing a successor to the EU-US Privacy Shield, pursuing this new authority now would be untimely and counterproductive. The Secretary appears to have the authority to indefinitely delay enacting these special measures as the executive order notes that in considering these special measures the Secretary should consider "significant adverse effect on legitimate business activities" as well as "the effect of any special measure on United States national security, law enforcement investigations, or foreign policy."

AT A MINIMUM, CREATE A REVIEW MECHANISM AND CRITERIA TO ASSESS PROGRAM EFFECTIVENESS

The Biden administration should scrap the KYC and AI usage reporting requirements. However, if it decides to proceed, it should, at a minimum, set out a timeframe, criteria, and mechanism to review the IaaS reporting regime to assess its effectiveness. A review should specify criteria to assess the regime's effectiveness, especially whether the system identifies and deters malicious actors or whether they change techniques to

circumvent the regime. Ideally, the U.S. government would develop some sort of baseline assessment or collection of data points to assess program effectiveness. Given that cyberattacks are likely to only grow in number, it will be very hard to specify the impact of this IaaS regime without criteria that will capture the impact of the new system. Ideally, a review would also provide another opportunity for U.S. stakeholders to provide feedback on how the regime is going and for the U.S. government to consider reforms to it.

FOCUS ON, AND FIX, PUBLIC-PRIVATE INFORMATION SHARING AND COLLABORATION

No one IT service provider has visibility into all the pieces of the puzzle in combating malicious cyber activity. This is why the Biden administration should focus on public-private information sharing and collaboration as it is key to identifying, preventing, and addressing malicious cyber activity. Better public-private information sharing and collaboration would allow a more complete picture of malicious cyber activity, rather than focusing on one actor providing a prescribed set of information that may not actually be useful. The goal should be to build collaborative mechanisms that enable cybersecurity professionals—regardless of their home agency or industry—to identify, track, and respond to threats as they arise, regardless of the infrastructure and services used.

U.S. government officials point to the need for enhanced collaboration and information sharing as part of the development of this IaaS reporting regime, yet the information the regime requires remains unclear and potentially not useful. Information shared for the purposes of disruption, mitigation, or future prosecution may or may not be the same information shared for the purpose of supporting an agency's analytic capability to understand the breadth and scope of such activity and actors, which could lead to better indicators for identifying future malicious activity.[15]

The Biden administration should focus on the need for enhanced and flexible information sharing and how this works (or doesn't) within existing cybersecurity laws, regulations, and information sharing mechanisms. For example, the liability safe harbor provided by the U.S.'s Cybersecurity Information Sharing Act of 2015 has several critical limitations:

- It cannot preclude the enforcement of applicable foreign law or civil action outside the United States, such as the application of the EU's General Data Protection Regulation (GDPR).
- It only applies when information exchanges are "conducted in accordance with" several specific technical requirements, including the advance removal of certain personal information, and use of a particular process within the Department of Homeland Security.
- It does not sufficiently incentivize the sharing of other categories of information beyond cyber threat information that may be useful in the context of malicious cyber activity.
- The scope of its preemptive and liability-shield provisions has not been fully tested.[16]

There are other barriers and challenges to information sharing that the Biden administration should address instead of creating a new and likely ineffective IaaS-specific reporting regime. For example, firms may be reluctant to proactively identify malicious activity on their platforms, as it could create risk, including increased liability. If, on the other hand, firms take no action, the abuse will continue, and the company may

incur a risk of liability to third parties from inaction. This dilemma disincentivizes some firms, particularly smaller providers, from conducting threat-hunting operations on their networks and services.[17] Furthermore, there are limited legal protections available to firms who act based on "false positives" and thereby disrupt legitimate use that is mistakenly identified as abuse. This is challenging given that malicious cyber actors go to great lengths to hide their activity within legitimate use, and so identifying abusive activities is often based on probabilistic judgments that may ultimately be incorrect.

The Biden administration should focus on these and other barriers to ensure existing cybersecurity information sharing and collaboration mechanisms are as effective as possible. Across government, existing mechanisms include the Enduring Security Framework, the Defense Cybersecurity Information Sharing Environment, InfraGard, the CCC, the Cybersecurity Risk Information Sharing Program, the National Cyber Investigation Joint Task Force, and the Joint Cyber Defense Collaborative (JCDC). The U.S. government (such as through intelligence agencies) and U.S. IaaS providers (and other IT service providers) have visibility into different parts of the problem. For example, the National Security Agency's membership of the Cybersecurity Collaboration Center (CCC) can turn intelligence-derived insights into actionable indicators and relevant information for other government agencies and industry stakeholders. It would be better for the Biden administration to focus on improving existing laws, regulations, and public-private collaboration rather than creating a new and problematic IaaS-specific cybersecurity framework.

Address Cloud-related Issues as Part of International Collaboration and Information Sharing on Cybersecurity

The United States should cover cloud-related issues as part of greater international information sharing and cooperation on malicious cyber activity. This could include discussions about creating similar legal frameworks for private firms to share information with government authorities on malicious cyber activity. It could also include joint cybersecurity advisories and multi-agency/national operational cybersecurity campaigns.

Cloud firms need market access, seamless data flows, and a clear legal framework to both share data and information and take preventative and remedial action in the event of cyberattacks. They need to be able to transfer data to learn from their global operations to better detect and respond to cyberthreats, whether these are in the United States, the European Union, or elsewhere. For example, in 2022, Google Cloud and other cloud firms defended themselves and their customers from the largest distributed denial-of-service attack on record—at 46 million requests per second—in part because they were able to identify it early on, as there were anomalous spikes in activity from IP addresses in four countries simultaneously: Brazil, India, Indonesia, and Russia. If Google and other global cloud providers lose the ability to collect and share security telemetry from around the world, it's going to be far more challenging to respond to cyberthreats and attacks in Europe and elsewhere around the world.[18]

The U.S. government has demonstrated the value of international cooperation on issues like ransomware and cyberattacks.[19] For example, the U.S. government, along with international partners, disabled Russian-affiliated malware that was being used to steal sensitive documents. This operation coincided with a lengthy joint cybersecurity advisory describing the malware and providing information to cyber defenders on how they could detect and disrupt the malware.[20]

However, there's still a lot of room for improvement in terms of domestic and international cooperation on malicious cyber activity, including creating a clear legal framework for private firms to share information with local and international cybersecurity authorities. For example, although there are scenarios under which local laws in the United States, European Union, and elsewhere allow private firms to share cyber threat information with governments, there is a lack of clarity about whether this is legally permissible. It raises the potential for financial and other legal penalties.

Legal barriers and uncertainty create a disincentive for firms to share information with government authorities. The United States should work with likeminded partners on this issue to ensure that cloud and other firms have a clear legal framework to share information with local and international authorities. Without a clear legal framework for information sharing for cybersecurity purposes (whether under privacy or cybersecurity laws and regulations), firms are likely to adopt a conservative legal and operational approach to data sharing to reduce legal compliance risks.

CONCLUSION

There are fundamental flaws in this proposed regulation. If the Biden administration does not revise or rescind these problematic provisions, it will create new trade and cybersecurity issues for U.S. cloud providers and put the U.S. cloud computing industry at a competitive disadvantage. The U.S. government should instead work with the private sector on how to improve existing laws, regulations, and public-private collaboration and how to create clear legal frameworks and mechanisms to improve both domestic and international collaboration and informaiton sharing on malicious cyber activity, including those that use IaaS cloud services.

Nigel Cory

Associate Director

ENDNOTES

[1] "Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities," U.S. Federal Register, https://www.federalregister.gov/documents/2024/01/29/2024-01580/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious.

[2] The National Security Telecommunications Advisory Committee, "Report to the President: Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors," September 26, 2023, https://www.cisa.gov/sites/default/files/2023-11/Draft%20NSTAC_Report_to_the_President_on_ADI_508c.pdf.

[3] "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," April 2, 2015, https://www.federalregister.gov/documents/2015/04/02/2015-07788/blocking-the-property-of-certain-persons-engaging-in-significant-malicious-cyber-enabled-activities.

[4] "Continuation of the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities," March 27, 2024, https://www.federalregister.gov/documents/2024/03/27/2024-06720/continuation-of-the-national-emergency-with-respect-to-significant-malicious-cyber-enabled#:~:text=These%20significant%20malicious%20cyber%2Denabled,effect%20beyond%20April%201%2C%202024.

[5] The National Security Telecommunications Advisory Committee, "Report to the President: Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors," September 26, 2023, https://www.cisa.gov/sites/default/files/2023-11/Draft%20NSTAC_Report_to_the_President_on_ADI_508c.pdf.

[6] Cybersecurity and Infrastructure Security Agency, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," February 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

[7] Ibid.

[8] "Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities," January 25, 2021, https://www.federalregister.gov/executive-order/13984.

[9] The National Security Telecommunications Advisory Committee, "Report to the President: Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors," September 26, 2023, https://www.cisa.gov/sites/default/files/2023-11/Draft%20NSTAC_Report_to_the_President_on_ADI_508c.pdf.

[10] Bank Secrecy Act of 1970. 31 U.S.C. § 5311 et seq. (1970)

[11] Cybersecurity and Infrastructure Security Agency, "Cybersecurity Information Sharing Act of 2015 Procedures and Guidance," October 15, 2021, https://www.cisa.gov/resources-tools/resources/cybersecurity-information-sharing-act-2015-procedures-and-guidance.

[12] Electronic Communications Privacy Act (ECPA)," Electronic Privacy Information Center, https://epic.org/ecpa/.

[13] Laurens Cerulus, "France wants cyber rule to curb US access to EU data," *Politico,* September 13, 2021, https://www.politico.eu/article/france-wants-cyber-rules-to-stop-us-data-access-in-europe/; "SecNumCloud," https://www2.itif.org/2021-secnumcloud-3.2.a-english-version.pdf; Nigel Cory, "Sovereignty Requirements in France—and Potentially the EU—Cybersecurity Regulations," December 10, 2021, https://www.crossborderdataforum.org/sovereignty-requirements-in-france-and-potentially-eu-cybersecurity-regulations-the-latest-barrier-to-data-flows-digital-trade-and-digital-cooperation-among-likemi/?cn-reloaded=1.

[14] Theodore Christakis and Fabien Terpan, "EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options," International Data Privacy Law, Volume 11, Issue 2, April 2021, Pages 81–106, https://doi.org/10.1093/idpl/ipaa022; "UK G7 Presidency Statement, Digital and Tech," December 21, 2021, https://www.g7uk.org/uk-g7-presidency-statement-digital-and-tech/.

[15] The National Security Telecommunications Advisory Committee, "Report to the President: Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors," September 26, 2023, https://www.cisa.gov/sites/default/files/2023-11/Draft%20NSTAC_Report_to_the_President_on_ADI_508c.pdf.

[16] Cybersecurity and Infrastructure Security Agency, "Cybersecurity Information Sharing Act of 2015 Procedures and Guidance," October 15, 2021, https://www.cisa.gov/resources-tools/resources/cybersecurity-information-sharing-act-2015-procedures-and-guidance; The National Security Telecommunications Advisory Committee, "Report to the President: Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors," September 26, 2023, https://www.cisa.gov/sites/default/files/2023-11/Draft%20NSTAC_Report_to_the_President_on_ADI_508c.pdf.

[17] The National Security Telecommunications Advisory Committee, "Report to the President: Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors," September 26, 2023, https://www.cisa.gov/sites/default/files/2023-11/Draft%20NSTAC_Report_to_the_President_on_ADI_508c.pdf.

[18] Emil Kiner and Satya Konduru, "How Google Cloud blocked the largest Layer 7 DDoS attack at 46 million rps," Google blog, August 18, 2022, https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps.

[19] "International Counter Ransomware Initiative 2023 Joint Statement," The White House, November 1, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement/; "United States, Australia, and the United Kingdom Sanction Russian Cyber Actor Responsible for the Medibank Hack," U.S. Treasury, Press Release, January 23, 2024, https://home.treasury.gov/news/press-releases/jy2041.

[20] "Hunting Russian Intelligence "Snake" Malware," Joint Cybersecurity Advisory, May 9, 2023, https://www.cisa.gov/sites/default/files/2023-05/aa23-129a_snake_malware.pdf.