GNI Comment on BIS Proposal Regarding Infrastructure as a Service

I. Introduction

The Global Network Initiative (GNI) is a multistakeholder organization that brings together more than 100 prominent academics, civil society organizations, tech companies, and investors from around the world. Members' collaboration is rooted in a shared commitment to the advancement of the GNI Principles on Freedom of Expression and Privacy, which are grounded in international human rights law and the UN Guiding Principles on Business and Human Rights (UNGPs). For over a decade, the GNI Principles and corresponding Implementation Guidelines have guided tech companies to assess and mitigate risks to freedom of expression and privacy in the face of laws, restrictions, and demands, including in politically sensitive contexts.

GNI thanks the Bureau of Industry and Security (BIS) for this opportunity to comment upon the notice of proposed rulemaking on "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities" ("Proposed Rule"). GNI appreciates BIS' focus on preventing cyber attacks. Many civil society organizations and other groups have been subject to malicious cyber attacks, a significant number of which have been perpetrated by authoritarian governments seeking to stifle freedom of expression.

GNI is concerned, however, that the Proposed Rule sends the wrong message about the best way to secure a free and open Internet and could have significant unintended negative consequences for civil society groups and marginalized individuals if implemented as proposed. In particular, GNI is concerned about the United States taking the approach that collection and compelled disclosure of personal information is a necessary precondition for cybersecurity. GNI believes that approach could undermine U.S. leadership in promoting a free, open, and global Internet and provide a pretext for authoritarian regimes to legitimize their own data collection and access. The Proposed Rule also would directly harm privacy rights by requiring mass collection and reporting of personal information that is disproportionate to any cybersecurity benefit it might serve, and would reduce access to services that enhance privacy and security for those who need them most.

II. Background

The White House first introduced the idea of requiring "that providers offering United States [Infrastructure as a Service] products verify the identity" of their customers in the January 19, 2021 Executive Order 13984, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activity." Nearly two years later, in December 2022, the White House tasked the National Security Telecommunications Advisory Committee (NSTAC) with developing proposed responses to prevent abuse of domestic infrastructure by foreign malicious actors. The NTSAC issued a 60-page report that, among other things, declined to endorse customer identification programs as an effective solution to the problem. Following

an Advanced Notice of Proposed Rulemaking, and Executive Order 14410, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," BIS issued the Proposed Rule.

The Proposed BIS Rule is largely premised on the idea that requiring Infrastructure as a Service (IaaS) providers to collect information about their users will allow the government to more effectively prevent abuse. By requiring IaaS providers to create a Customer Information Program, the Proposed Rule would require the collection of a significant volume of information about IaaS customers. Key collected data would include:

- Name;
- Address;
- Means and source of payment for an account;
- Email address;
- Telephonic contact information;
- IP address used for access and administration, as well as date and time of such access or administrative action.

Companies that provide U.S. IaaS services would be required to collect this data, verify it using either documentary or non-documentary means, and retain this data for non-U.S. persons for two years after the relevant account was closed or was last accessed. U.S. providers of IaaS services would also be required to pass these requirements on to their foreign resellers.[1]

Additionally, to implement the applicable Section 4.2(c) of E.O. 14410 under the Proposed Rule, the Department of Commerce is empowered to require U.S. IaaS services to report 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". This includes detailed and personal information including their identity, contact, address, means of payment, and information about the AI training run.

III. Necessity and Proportionality

By requiring U.S. Infrastructure as a Service providers to gather and retain data about their customers as a condition for providing service, the Proposed Rule would result in large collections of personal data that are inconsistent with privacy rights. In addition, GNI is concerned that the data collection required by the proposed rule would not be proportionate to any benefit offered by the rule and thereby risk violating international human rights law. Iaas providers forced to keep troves of customer data are likely to be subject to government orders to turn over this data, whether in the United States or elsewhere, and to cybersecurity attacks

[1] The Proposed Rule would allow for a possible exemption to the data collection requirement that would be granted and revoked at the discretion of the Secretary of Commerce, in consultation with other government leaders. GNI does address that proposed exemption provision here, other than to note that it does not negate the concerns that it has with the underlying data collection requirement, particularly given the procedural and substantive challenges inherent in the proposed exemption process.

seeking to obtain and compromise this data. Failures to comply with specific provisions in the proposed rule may risk liability for individual employees at the level of senior management who are designated as responsible (Proposed Rule § 7.306). Service providers' efforts to resist illegitimate orders or malicious cyberattacks will not always be successful, which is why well-established privacy principles dictate against the unnecessary collection and retention of such data.

Similarly, the requirement on U.S. IaaS services to report to the Commerce Department when a foreign person transacts with them to train a large AI model with *potential capabilities that could be used in malicious cyber-enabled activity* puts private data at risk*. Moreover, the compelled disclosure of this data directly conflicts with the Stored Communications Act of 1986 which, under U.S. Code § 2702, prohibits remote communications services - i.e. services that provide the public "computer storage or processing services by means of an electronic communications system" - from disclosing information "pertaining to a subscriber or customer [..] to any governmental entity" in the absence of legal process. The Proposed Rule currently does not offer an explanation of how the compelled disclosure requirement may be harmonized with the existing statutory provision.*

These problems are compounded by the scope of services that may be subject to the Proposed Rule. While the Proposed Rule defines the targeted services as those that provide "processing, storage, networks, or other fundamental computing resources, and with which the consumer is able to deploy and run software that is not predefined," (Proposed Rule § 7.301) the Department's commentary indicates that it will interpret that definition broadly to include "services such as content delivery networks, proxy services, and domain name resolution services," (89 Fed. Reg. 5702). Such services are widely used and fundamental to free expression, particularly in countries with authoritarian regimes. Virtual Private Networks (VPNs), for example, are one form of "proxy service" that has been recognized as protecting individuals' privacy and security in navigating the Internet, especially under authoritarian regimes in Russia, China, and the Middle East. Likewise, "domain name resolution services" are part of the fundamental architecture of the Internet that has long been governed by multistakeholder processes. To the extent these types of services are potentially in scope of the Proposed Rule, the amount of private data that would be collected could be unprecedented. GNI strongly recommends that the Department reconsider the Proposed Rule in light of the significant potential implications for privacy worldwide.

IV. Privacy and Security for Civil Society Groups

GNI is also concerned that the Proposed Rule will harm privacy and security interests by discouraging the use of vital services, particularly among the most at risk groups. Civil society groups and marginalized individuals regularly sustain cyber attacks and other forms of digital scrutiny and assault. Fortunately, governments and private companies have increasingly recognized those risks and responded by providing or supporting free or subsidized services that enhance privacy and security. For example, the Joint Cyber Defense Collaborative (JCDC), in

partnership with industry and civil society, recently launched a suite of resources - including those from private industry - to help civil society organizations bolster their cyber defense and resilience. Some of those resources could potentially be in scope of this Proposed Rule.

By making the disclosure of personal data a condition for accessing U.S. infrastructure services, and creating the risk that such data will be compromised, the Proposed Rule would have the unintended consequence of discouraging civil society groups from using such services. Faced with the requirement to turn over sensitive data as a condition of service, many civil society groups or other marginalized individuals will instead choose not to use U.S. IaaS services. Civil society groups and others who turn away from U.S. IaaS providers will likely find themselves forced to accept options that are less secure and that less effectively protect their privacy. While they may thus avoid the proposed data collection, these individuals may well be exposed to a greater risk of abuse. Alternatively, they may abandon or curtail their online activities. To the extent that it discourages civil society groups and marginalized individuals from using U.S. IaaS services in this manner, the Proposed Rule thus could undermine the United States' efforts to advance democratic values through safe and private access to the Internet around the world.

The Proposed Rule also will limit the availability of such services in the first place, by creating new and costly compliance requirements for U.S. IaaS providers. This poses a particular challenge in the context of services that are provided for free or on a subsidized basis. Without corresponding revenue to cover the costs of these services, companies that offer free or low-cost services to civil society groups are likely to reduce or withdraw these services. Indeed, such providers may have little choice, as the Proposed Rule simply may make it cost prohibitive to offer services that incur substantial compliance costs.

This is not a hypothetical concern. India provides a ready example of infrastructure companies leaving a market in the face of burdensome regulatory requirements that made continued service infeasible. GNI is concerned that implementation of the Proposed Rule similarly would result in civil society groups and marginalized individuals losing access to valuable technologies that support free expression and enable the safe pursuit of democratic values. The United States' interests globally will suffer in this event, not to mention the direct consequences for civil society groups, dissidents, journalists, and other marginalized groups. GNI worries, for example, that reduced access to these services could ultimately contribute to the mistreatment of political dissidents, meddling with elections, or the stifling of free expression.

V. US Leadership on Internet Freedom undermined

The U.S. government has long led global efforts to preserve and expand the Internet as an open, free, global, interoperable, reliable, and secure forum that supports democratic principles, human rights, and fundamental freedoms. Sixty global partners gathered at the White House to affirm their support for the Declaration of the Future of the Internet, which includes commitments to "secure and protect individuals' privacy, maintain secure and reliable connectivity, resist efforts to splinter the global Internet, and promote a free and competitive

global economy." The Biden Administration's Executive Order from 28 February 2024 on the transfer of Americans' sensitive personal data to countries of concern is another example of the United States' support for trusted free flow of data while ensuring protection of individuals' privacy. Fundamental to the US government's effort to promote an open Internet has also been defending it against digital authoritarianism. GNI also appreciates the government's commitment to opposing censorship by highlighting the importance of "safeguarding individual privacy" in the 2023 National Cybersecurity Strategy in implementing "EO 13984, 'Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities".

However, GNI fears that the Proposed Rule, and specifically the requirement that US providers collect and disclose personal information as a condition of providing Internet infrastructure services, will be perceived as a departure from the United States' support for a free and open Internet and undermine US leadership on Internet freedom. Such a perceived change in the United States' attitude towards safe and private access to the Internet may encourage other nations to press forward with efforts to collect information about infrastructure usage—or Internet usage more generally—within their jurisdictions. The United States must continue to push back on these efforts by giving a clear voice to the need for a free, open, and global Internet. The adoption of policies that call into question the United States' commitment to these important principles is likely to embolden authoritarian states and weaken the United States' ability to credibly push back on future constraints on Internet privacy and security that they impose.

VI. Conclusion

The United States has sought to articulate a vision of the future of the Internet that is "open, free, global, interoperable, reliable, and secure" and to ensure that the Internet reinforces democratic principles and human rights and fundamental freedoms.[2] Mandating verification of identity as a condition to using a wide range of Internet services, including those historically governed by a multistakeholder model, is fundamentally inconsistent with that vision.

As BIS works to reduce the abuse of IaaS services by malicious cyber actors, GNI urges caution in ensuring that the chosen approach does not have the unintended consequence of harming civil society organizations and marginalized individuals around the world. GNI encourages BIS to instead build upon the United States' existing commitment to a free, open, and global Internet that enables free expression and the advancement of democratic values. To do so, BIS should:

- Carefully evaluate the risk of the Proposed Rule causing unintended consequences for civil society groups and marginalized individuals across the globe;

[2] As summarized here, these initiatives to advance a free and open Internet have played an important part in the United States' broader efforts to advance democracy and human rights.

- Work with relevant stakeholders to consider more constructive approaches to address abuse of US infrastructure services, focused on the malicious activity rather than the collection and compelled disclosure of personal information;
- Develop a revised regulatory approach that avoids the collection and reporting of substantial information about individuals and civil society groups using U.S. IaaS services and ensures that privacy- and security-enhancing services remain available to individuals and civil society groups around the world.

GNI encourages BIS to consider these recommendations as it takes further steps in this rulemaking process. GNI looks forward to further engagement on preventing abuse of Internet infrastructure in a manner that advances democratic principles and freedom of expression around the world.