THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

NSTAC REPORT TO THE PRESIDENT

Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors

Date: TBD

Table of Contents

Figures

Executive Summary

Introduction

In December 2022, the Executive Office of the President (EOP) tasked the National Security Telecommunications Advisory Committee (NSTAC) with a new study on "Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors."[1] The NSTAC established a committee to investigate and report on what voluntary actions key internet ecosystem companies, notably hosting providers, infrastructure as a service (IaaS) providers, internet service providers, telecommunications providers, domain name system service providers, and network and endpoint security providers, are currently taking to prevent or mitigate the abuse of domestic infrastructure (ADI) by foreign malicious actors. The EOP also requested the committee investigate factors that are creating opportunities, challenges, and barriers—including financial, legal, technological, and human — that may be assisting or preventing public and private stakeholders from systematically addressing malicious actor ADI. After a series of briefings and committee analysis, the NSTAC is proposing actionable recommendations that can improve this shared public-private effort to collaborate and combat ADI "while maintaining a voluntary, private sector-driven operational model," as the EOP directed.[2]

Study Scope and Overview

Study Scope

"Abuse" means to "put to a wrong or improper use." In the context of "cyber operations," this abuse could include everything from foreign-based nation-state actors seeking to infiltrate U.S. government systems to financially motivated cybercriminals conducting credential harvesting and phishing attacks. While all briefers consistently identified abuse as a significant issue, government briefers could not articulate with specificity: (1) the type of abuse they were most concerned with or sought to address; (2) the tactics of malicious actors; or (3) where they had the greatest challenges. However, industry briefers were clear that the abuse prevention techniques they employ seek to prevent or mitigate all types of abuse, and companies often cannot determine with certainty whether users of their products are foreign or domestic or if the users' operational goals are malicious or legitimate. In essence, "abuse is abuse," whether carried out by Americans or foreigners, and whether the actors are in the United States or in a foreign country. Accordingly, much of the guidance in this report about "abuse of domestic infrastructure by foreign malicious actors" is generally applicable to prevent ADI, regardless of the malicious actors' country of origin.

In addition, a common question raised to briefers by the committee was whether it is possible to tell the difference between a foreign and a domestic actor. Interestingly, whether the briefers represented a government agency, a private company, or a stakeholder organization, there was no easy or consistent answer to this question. If today's technology allowed infrastructure providers to identify the nationality and location of

[1] See EOP scoping paper in Appendix A.

[2] Ibid.

malicious actors, or if all users would truthfully declare their nationality and current location, then the private sector could easily separate foreign actors overseas from U.S. persons. Further, knowing whether the malicious actor is foreign or domestic does help in deciding which government agencies get involved and which legal authorities are available to disrupt, investigate, and prosecute the actor.

There is a widespread perception that attribution in general is becoming easier due to the growth of the threat intelligence ecosystem and more regular instances of companies and governments publicly calling out specific alleged threat actors. There are many factors, however, that make it harder for defenders in government and in the private sector to have insight into actor identities in the context of routine and highly automated online business transactions at scale in pre-event scenarios. This is different than attribution after an event has occurred, which is more attainable, but is also often time consuming, costly, and labor-intensive. Thus, the committee found that the private sector cannot quickly and accurately distinguish between foreign and domestic actors.

The committee recognizes the U.S. government's inclusion of a strategic objective on preventing abuse of U.S.-based infrastructure in its recently released National Cybersecurity Strategy[3] and corresponding Implementation Plan.[4] However, U.S. government briefers did not articulate a clear overarching U.S. government strategy with respect to addressing ADI. The committee heard from multiple government agencies, each with its own distinct mission, objectives, tools, and authorities. The committee found that in the absence of an overarching strategy on countering ADI, including consideration as to when systemic issues such as ADI might take precedence over more narrowly tailored operational objectives, there is risk of unintentional overlapping and competing priorities and interests among the agencies with relevant responsibilities. This can complicate efforts to work with the private sector in addressing ADI.

The NSTAC notes that any U.S. government strategy on ADI must be multi-faceted and ever evolving given the dynamic threat environment. Just as malicious actors engage in continuous action to achieve their desired ends, public and private stakeholders must engage in continuous action to keep pace with or get ahead of malicious activity. The briefings to the committee showcased significant human and technological innovations in cybersecurity that complement innovations in technology products and services over the last few decades, but there is widespread recognition and agreement that there is no security "silver bullet" or one best practice to combat ADI. Continuous action and a layered approach are required to address cyber threats from ADI over the long term. Today's best practice may not protect against tomorrow's vulnerability, which requires any U.S. government policy, investment, and action to reflect this continuously evolving, layered approach.

---

[3] "National Cybersecurity Strategy," The White House, March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[4] "National Cybersecurity Strategy Implementation Plan," The White House, July 13, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.

Report Summary

Section 1, *Background,* provides an overview of the types of abuse and threat actors covered by the report. This section describes how threat actors conduct malicious cyber activity using commercial products, platforms, services, or systems hosted on infrastructure located inside the U.S. or managed by U.S. companies that are under the jurisdiction of the U.S. (hereinafter "domestic infrastructure"). Both nation-state-backed actors and financially motivated cyber-criminal organizations engage in ADI to achieve speed and scale in their operations and elude cyber threat analysts and government investigators.

Section 2, *Current Efforts to Mitigate ADI,* provides an overview of current efforts and best practices by public and private stakeholders to mitigate ADI, and highlights the importance of certain best practices for mitigating abuse as well as in collaboration and information sharing. Together and independently, the U.S. government and a range of stakeholders, including companies, academia, non-profits, and others, have developed proficiency and proven mechanisms for working together to share expertise and mitigate ADI. This voluntary, collaborative defense-in-depth approach serves as the foundation for government and industry efforts to deal with existing and emerging cyber threats and informs risk management approaches, including combatting ADI.

Section 3, *Key Issues,* focuses on several key issues raised and discussed in numerous briefings, notably: (1) the increasingly global set of legal requirements companies face regarding the collection, use, retention, and destruction of the data they process or control; (2) resource barriers, including the need for better detection tools and greater accessibility for small and mid-size enterprises; (3) challenges stemming from reselling infrastructure, especially to foreign entities; and (4) proposed know-your-customer (KYC) requirements outlined in Executive Order 13984 (EO 13894), *Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities.* [5]

Section 4, *Recommendations,* proposes key actionable recommendations to the U.S. government to work with industry to mitigate ADI.

Key Findings

The NSTAC reached the following conclusions based on its evaluation of the extensive input of facts and expert opinions from a variety of briefers:

- **Finding 1:** A multi-faceted strategy is required to combat ADI. No singular action or approach will fully address the challenge on its own. Rather, a layered approach is needed to combat ADI, requiring effective strategic direction within the U.S. government, and employing multiple lines of effort and alignment across government agencies, industry, and civil society. While many facets to combat ADI are

[5] Executive Order No. 13984, "Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities," The White House, 86 FR 6837 (January 19, 2021), Federal Register: Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities.

currently in place or under development, a strategic, coordinated approach is essential to help unify these efforts.

- **Finding 2:** Combating attacks from our adversaries, including those perpetrated using domestic infrastructure, requires continuous and iterative international cooperation and an understanding of the constraints of myriad existing legal frameworks.

- **Finding 3:** Solutions to combat ADI should address overall abuse, whether conducted by domestic or foreign actors. 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. Often, malicious foreign activity is already disguised by threat actors to look like domestic activity. Efforts to impose additional requirements targeting foreign rather than domestic actors will provide even greater incentives for malicious foreign actors to use tactics that make them appear to be domestic actors.

- **Finding 4:** The overall prevalence and scale of ADI is not well understood or documented. While briefings established that malicious foreign actors abuse domestic infrastructure, the committee was not briefed on any rigorous studies analyzing the tradeoffs of potential policy and technical approaches that attempt to distinguish between domestic and foreign abusers. The committee also was not provided with any identifiers or indicators specifically tied to malicious foreign actors engaged in ADI. These limitations made it difficult for the NSTAC to evaluate the overall scope and impact of the subject of the tasking, as well as estimate the value of potential recommendations and solutions.

- **Finding 5:** A requirement for IaaS providers to verify the identity of foreign customers (i.e., KYC) through collection and retention of national identification information and other information as proposed by EO 13984[6] would be unlikely to decrease ADI by malicious foreign actors using domestic infrastructure. Further, such requirements may result in additional unintended consequences, including increasing friction with key U.S. allies, whose cooperation is critical in addressing global cyber threats.

- **Finding 6:** Multiple measures considered to be best practices for fraud and abuse detection and prevention are being utilized today by some infrastructure providers. Elevating the importance of these practices and promoting their adoption with all providers, including small and mid-size enterprises, should help to mitigate ADI. Adoption of such practices should inform the basis of the Commerce Department's potential implementation of EO 13984.[7]

- **Finding 7:** Focused information sharing and collaboration between the private sector and the government, as well as within the private sector, is needed to better understand the scope and scale of

[6] The White House, Executive Order No. 13984, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber- Enabled Activities."

[7] Ibid.

ADI and to adequately address it. The NSTAC recognizes that some mechanisms already exist to enable this collaboration and they should be leveraged to address this issue more effectively.

- **Finding 8:** There are real and perceived barriers for private sector companies (companies) to share threat information with one another as well as with the U.S. government. In addition to resource constraints, these barriers often involve legal and reputational concerns, including liability issues and privacy constraints from both domestic and international laws. These factors create disincentives, notably with small and mid-size enterprises, to determine what harmful activities exist on or emanate from their networks.

- **Finding 9:** There is great promise in technology to enhance our collective ability to combat ADI, such as through privacy protection mechanisms and privacy-enhancing technologies that can support greater information sharing. There is also potential for additional applications, such as artificial intelligence (AI) and machine learning, to boost the efficiency of efforts to detect, mitigate, and prevent or disrupt ADI.

- **Finding 10:** U.S. companies play an important role in combatting malicious cyber activities. Rather than seeking to prevent foreign actors from using U.S. infrastructure, a task the NSTAC concludes is infeasible (as stated in previous findings), U.S. companies should be empowered to prevent, detect, investigate, disrupt, and mitigate the harm from those activities more effectively.

- **Finding 11:** Analysis would be needed before the U.S. government considers applying the measures employed in the Bank Secrecy Act[8], specifically the banking sector suspicious activity report (SAR) program, for cybersecurity purposes. While there may be the potential to assist in combatting ADI, there are significant differences between the financial and information technology sectors that need further study. Specifically, the committee did not receive information to assess what activities would be deemed sufficiently suspicious to trigger reports, how that information would support efforts to combat ADI, and how that data would be protected to address inevitable privacy concerns, both domestic and foreign.

Summary of Recommendations

Over the course of outlining the overall opportunities and challenges associated with preventing ADI, the NSTAC identified six actionable recommendations, summarized here, and described more fully in Section 4.

Recommendation 1: The NSTAC recommends that the president direct the Office of the National Cyber Director to develop a strategy for combating ADI that recognizes the need for and establishes a long-term, multi-faceted approach to combat ADI as part of its implementation of the National Cybersecurity Strategy.[9]

Recommendation 2: The U.S. government, working through the Cybersecurity and Infrastructure Security Agency's (CISA) Joint Cyber Defense Collaborative and the National Security Agency's (NSA) Cybersecurity

[8] Bank Secrecy Act of 1970. 31 U.S.C. § 5311 *et seq*. (1970). The Bank Secrecy Act | FinCEN.gov

[9] The White House, "National Cybersecurity Strategy."

Collaboration Center, should create an operational working group that includes relevant private sector providers and key government representatives to focus on enhancing tactical collaboration to address ADI.

Recommendation 3: The U.S. government, through the National Institute of Standards and Technology and other relevant departments and agencies, should conduct a pilot program to test the practical application of privacy enhancing technologies to accelerate the development of at-scale data sharing and analysis of threats to domestic infrastructure.

Recommendation 4: The U.S. government should create a public-private task force to develop a framework that outlines best practices to mitigate ADI, including for managing reseller relationships. This framework will serve as a guide to enhance security practices of technology providers across the ecosystem and could also serve as the basis for the Commerce Department's potential implementation of Section 1(c) of EO 13984,[10] which enables the Commerce Department to exempt an IaaS provider from the Section 1(a) identity verification requirements.

Recommendation 5: The U.S. government, working through CISA, the NSA, the Federal Bureau of Investigation, and the Department of State, should develop a strategy to share intelligence with international partners regarding U.S. government concerns about abuse of virtual resources, and encourage joint operation, provide feedback to infrastructure providers, and facilitate collective defense.

Recommendation 6: The U.S. government, working through CISA and the Department of Justice, should work with the appropriate entities to coordinate the development of a set of recommendations with the private sector to update and enhance the Cybersecurity Information Sharing Act of 2015,[11] which is set to expire on September 30, 2025.

[10] The White House, Executive Order No. 13984. "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities."

[11] Cybersecurity Information Sharing Act of 2015, 6 U.S.C. §§ 1501–1510 (2015), https://law.justia.com/codes/us/2015/title-6/chapter-6/subchapter-i/.

1. Background

1.1. Introduction

"Abuse of domestic infrastructure" (ADI) refers to malicious actors' committing cyberattacks using commercial products, platforms, services, or systems hosted on infrastructure located inside the United States or managed by companies under the jurisdiction of the United States (hereinafter "domestic infrastructure"). Both nation-state-backed actors and financially motivated cybercriminal organizations abuse domestic infrastructure in a number of ways to achieve speed and scale in conducting malicious cyber activity while eluding cyber threat analysts and government investigators.

Nation-state actors, for example, engage in a broad swath of malicious cyber activities, including those that seek to steal trade secrets, influence geopolitics, or corrupt, destroy, exfiltrate, or ransom systems or data. Nation-states usually try to hide their identity and may attempt to shift the blame for their activities to hacktivists, cyber-criminal organizations, or other countries. By contrast, cyber-criminal organizations may work independently or with the cooperation or tacit approval of malicious nation-state actors. Organized cyber criminals are engaged in many diverse types of attacks, including fraud, malware, intellectual property theft, ransomware, denial of service (DoS) attacks, botnet attacks, phishing, business email compromise, and more.

ADI presents many challenges and obstacles for the U.S. government's use of traditional tools, procedures, and capabilities for tracking, preventing, and disrupting malicious cyber activities. This reality has fueled urgency in finding additional ways to make domestic infrastructure less hospitable to malicious actors and focus attention on what further actions the private sector can take given the private sector's visibility into its infrastructure and operations. Proposed rules, such as those required by Executive Order 13984 (EO 13984), *Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities.*[12] attempt to put into place extensive data collection mechanisms, in this case like the "Know Your Customer" (KYC) financial sector requirements. Implementing the EO's proposed KYC requirements is envisioned to both make it more difficult for some malicious actors to procure domestic infrastructure and to increase the potential availability of records that could be useful for investigations.

Since most malicious actors route their cyber activities through at least one intermediary and not directly from the attacker to the victim, several categories of virtual resources can be used for purposes that were not intended by their creators and vendors. Moreover, those using virtual resources for legitimate purposes may become victims themselves, finding their infrastructure compromised for use in malicious activities.

The virtual resources – including virtual private servers, remote storage, and domain hosting – that encompass "domestic infrastructure" for the purposes of this report offer both legitimate and malicious users several

[12] Executive Order No. 13984. "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities," The White House, 86 FR 6837 (January 19, 2021), Federal Register: Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities.

advantages, notably flexibility, scalability, and speed, at low cost. Accessing domestic virtual resources is simple, with some providers even offering them free of charge. 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). This ease of access and procurement makes it difficult for providers to differentiate between malicious actors and legitimate users.

Malicious actors may use virtual resources to perform activity on victims' machines, store exfiltrated victim data, host malicious payloads (including the components of a cyberattack), and communicate with victims as well as other malicious actors. Moreover, virtual resources can be commoditized by malicious actors and resold to others who can launch attacks without significant resources or technical knowledge. Threat actors can rent malicious services, such as ransomware-as-a-service or malware-as-a-service, and even buy access to victim organizations via access brokers. Consequently, the same modern efficiencies and conveniences of virtual resources that benefit legitimate users also benefit our adversaries.

Virtual resources enable malicious actors to establish new infrastructure quickly, within hours or minutes, which they can then rapidly dismantle after use, helping them to stay ahead of defenders and investigators. They can then repeat the same cycle rapidly through other providers or other fraudulent or compromised accounts. Virtual resources also facilitate establishing larger networks of multi-layered intermediaries that complicate tracing traffic back to the malicious actors' origin.

The challenge of combatting ADI involves the technologies, infrastructure, and interests of many companies across the technology ecosystem. This ecosystem is vast, involving hosting providers, internet service providers (ISP), virtual private servers (VPS), content delivery networks (CDN), virtual private networks (VPN), and other components of infrastructure as a service (IaaS), to name a few. Private sector entities generally operate these components and malicious actors can leverage these resources to conduct illicit activity and often use a mix of virtual resources that may be governed by U.S. and non-U.S. laws and regulations. Combatting ADI becomes even more complicated when offerings are sold by resellers, especially when those services are purchased from other resellers. This ecosystem is summarized in more detail in an appendix to this report.[13]

1.2. ADI in Action

Threat actors can abuse domestic infrastructure through a wide range of techniques, exploiting technical weaknesses in hardware and software through a variety of methods. It is not possible for a single entity in the ecosystem to have a comprehensive view of the full range of a threat actor's malicious activity. However, each virtual resource provider has a unique vantage point at different stages of malicious activity.

To augment visibility and protect against malicious activity, virtual resource providers and potential victims can deploy a variety of security solutions, such as those mandated for government agencies in Executive Order 14028 (EO 14028), *Improving the Nation's Cybersecurity*, including endpoint detection and response, zero trust

[13] See Appendix B for more information on the different types of virtual resources that can be subject to abuse of domestic infrastructure (ADI).

architecture, and log management.[14] These technologies can be applied to endpoint computers, virtual and physical servers, authentication servers, networks, and cloud containers. When operators of virtual resources and targeted machines leverage modern security solutions – such as cloud-native technologies – they can have visibility into or block the threats that traverse their systems.

For example, the simple scenario of malicious activity illustrated below shows what actions a threat actor may take, and the information various providers may see from those actions. If a threat actor intends to send a U.S.-based victim a piece of malware via email, the threat actor first needs to acquire a command and control (C&C) server, which will enable the threat actor to communicate with the malware once installed on the victim's computer. The threat actor might register a domain name with a U.S.-based registrar. The threat actor also might set up an email address utilizing a domain name system (DNS) mail exchange record and point the domain names to a mail server hosted by a hosting provider. From there, the threat actor can deceive or coerce a victim to take a compromising action, such as clicking on a link in an email or opening a file attachment. The intention of such an action is to launch some sort of malicious payload, which can be malware or, increasingly, the running of a script on a victim's endpoint. Once the payload is deployed, a threat actor may be able to take subsequent actions, such as deploying remote access tools, exfiltrating data, or encrypting data using ransomware, unless these malicious activities are prevented by security solutions.

[14] Executive Order No. 14028. "Improving the Nation's Cybersecurity," The White House, 86 FR 26633 (May 12, 2021), Executive Order on Improving the Nation's Cybersecurity | The White House.

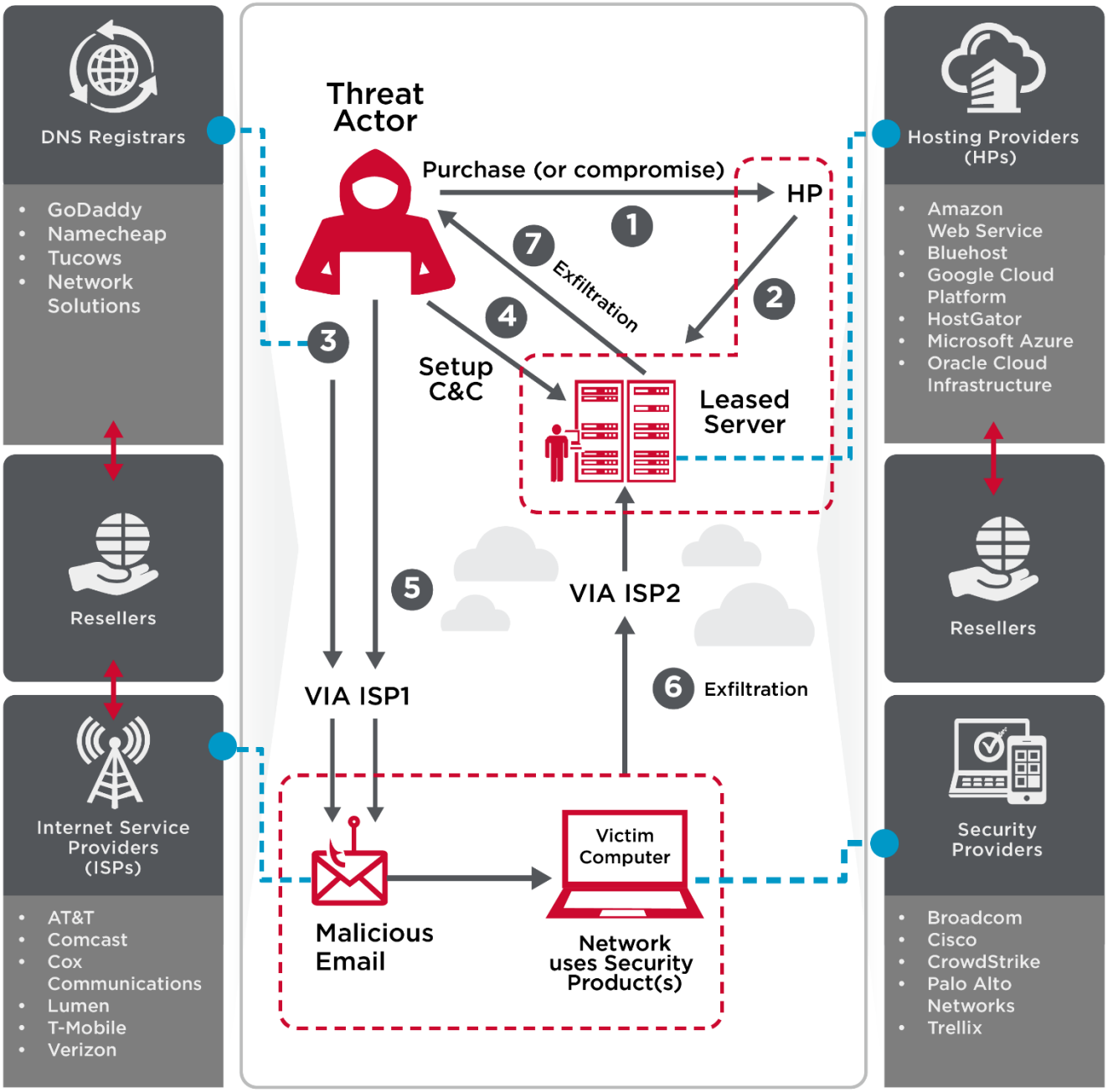

Figure 1: ADI in Action[15]

In the illustrated example, a variety of different providers might have access to various activities from different vantage points and have different abilities to prevent or disrupt the activity.

- If the threat actor purchased services from a hosting provider, the hosting provider may see the threat actor's billing details, where the threat actor logged into the hosting provider's system, and any other C&Cs purchased by the threat actor on the hosting provider's infrastructure.

- The domain name registrar will see account information, such as contact information and payment details, of the registrant of the domain name(s) associated with the email, pointing to the server hosting the malware, or pointing to the server to which exfiltrated data is being sent.

- The ISP may see the metadata of the transaction (e.g., a victim's computer internet protocol (IP) 1.2.3.4 used source port 34567 to speak with a hosting provider's IP 5.6.7.8 at port 443 and sent approximately 1GB of information on 5/5/2023 at 11:22 a.m.).

- The hosting provider has the ability to see the victim's IP, and the threat actor's source IP (the source IP is where the threat actor accesses the C&C, which may be a VPN). In limited circumstances, the hosting provider may be able to see content exfiltrated from the victim's computer, but most often content data is not visible.

- A reseller of virtual resources will see the registration information, including contact and payment information, of the account owner of the domain name or hosting resources.

- The security providers used by the victim's network will have logs related to the attempt to deploy the payload and may have the ability to filter the malicious content or prevent data exfiltration. The network security provider used by the victim will see domain names, DNS records, email transaction logs, and associated IPs used as the threat actor's infrastructure.

While all this information is valuable for those best situated to disrupt malicious activity, such as individual providers or U.S. government agencies, what should be most evident is that no one service provider has visibility into all of the pieces of the puzzle, suggesting that information-sharing and collaboration is key to prevention and disruption.

[15] NOTE: The providers listed are only a sample of companies that provide these services, and these companies may also provide additional services than those portrayed above. The network connections between a threat actor and various providers typically consist of VPN connections and intermediate hop nodes, obscuring actual network locations. The diagram omits that detail for simplicity of presentation.

2. Current Efforts to Mitigate ADI

2.1. Introduction

The private and public sectors have long collaborated to develop technical measures and collaborative approaches to address cyber threats facing the nation. These efforts seek to keep pace and stay ahead in a dynamic threat environment that responds to the continuous changing techniques of malicious actors to achieve their desired ends. As noted in the National Cybersecurity Strategy, "malicious cyber activity has evolved from nuisance defacement to espionage and intellectual property theft, to damaging attacks against critical infrastructure, to ransomware attacks and cyber-enabled influence campaigns designed to undermine public trust in the foundation of our democracy."[16]

As the malicious activity has evolved, so have the techniques. An example of this is the use of ephemeral mechanisms and infrastructure, including VPN tunnels, voice-over-internet-protocol (VOIP) telephone numbers, pre-paid credit cards, pay-as-you-go cloud storage systems, and compute nodes (such as containers and virtual machines). This technique effectively obfuscates malicious cyber activity across a wide range of technologies and providers. Consequently, the job of mapping malicious activity across all these modern processes has become more challenging. Even when detection is successful, the resources and infrastructure may be gone—torn down or abandoned—and the actor may have already moved to a new set of ephemeral resources. Threat actors move quickly, and time is of the essence for detecting, mitigating, and responding to ADI.

Despite significant innovations in cybersecurity that complement innovations in technology products and services over the past few decades, there is widespread recognition that there is no security "silver bullet" and therefore a layered and constantly evolving approach is needed to address cyber threats. Together and independently, the U.S. government and a range of stakeholders, including companies, academia, non-profits, and others, have developed expertise and best practices, and have built structures for sharing that expertise. It is critical to acknowledge that these "defense-in-depth" as well as "defense-in-breadth" approaches serve as the foundation for government and industry efforts to deal with existing and emerging cyber threats and informs risk management approaches, including combatting ADI.

2.2. Industry Best Practices

Many companies already make significant investments in people, processes, and technologies to deter, detect, and disrupt malicious activity. Many companies have the incentive and resources to make these investments given their interest in promoting ecosystem security, providing reliable service, avoiding the financial loss of fraudulent behavior (i.e., non-payment for services, which often accompanies abusive behavior), and avoiding reputational and financial harm. In addition to the range of efforts that companies undertake to improve cybersecurity generally and address cyber threats, multiple briefers highlighted common practices to specifically

[16] "National Cybersecurity Strategy," The White House, March 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

address abuse, such as fraud,[17] account takeovers, or distributed denial-of-service (DDoS) attacks. These practices include efforts to deter, prevent, detect, and mitigate ADI.

In their briefings, companies shared multiple mechanisms they employ to combat ADI. Given the diverse circumstances in which ADI may occur, these efforts vary in different stages and from service to service. Risk-based approaches are deployed to address these challenges, with different processes depending on the likelihood and nature of potential abuse. Processes for identifying fraud at the point of account creation, for example, are not the same as those needed for detecting a malicious takeover of an existing, legitimate account. While these measures may not eliminate the risks of abuse, they play a significant role in reducing the attack surface and raising the costs for the malicious actors that abuse U.S. infrastructure. It is also worth noting that the ability to employ best practices may be resource dependent, which can create access and capability challenges for small and mid-size companies.

2.3. Preventing Abuse

Processes to prevent ADI typically begin at account creation. Many companies introduce processes during registration that can make it harder for an illegitimate customer to acquire services by causing "friction," that is, slowing or limiting legitimate account creation. For example, companies may implement controls to block automated account creation, build automated rules in the sign-up flow to detect and block known bad actors or fraud patterns, or partner with payment processors to prevent actors from creating accounts using fraudulent identities or payment methods. Some companies noted that they initially collect limited customer information that can be used to support identity verification, such as name, address, email address, and/or phone number. Identifying information that does not line up—such as a mailing address that is in a different location from the IP address and/or the telephone number being used—may result in denial of account creation because it is an indicator of a potentially fraudulent or abusive customer.

Continuing through the lifecycle of the relationship with the customer, providers may take steps to assess the trustworthiness of customers and ensure that customer behavior aligns with their terms of service. Some providers enforce limitations, or quotas, on customer allocation of compute resources, especially for new customers and for any customer accounts that may display unusual behavior. This can include providing services to new customers incrementally, until they are able to build trust with the provider. Providers may even choose to moderate customer use of a service depending on their type of payment instrument.

Companies also described mechanisms for identifying and addressing possible account compromise to help prevent the abuse of a legitimate account for malicious purposes. For example, tools to identify and prevent

[17] Fraud in this context can include efforts to use illegitimate payment mechanisms, falsify identity, or otherwise defraud the provider.

credential stuffing attacks[18] may help prevent an account from being compromised, while automated tools that search for user anomalies or other indicators of compromise might help remediate account takeover before there is an opportunity for ADI.

2.4. Detecting Abuse

Some companies detailed a process for using machine learning (ML) to detect abuse. This approach involves gathering a large amount of historical data, tagging those data sets that were later determined to be associated with a fraudulent or abusive customer, and then building ML models that either deny account creation, or if allowed, assign a "trust" determination that may include assigning a "score" based on this probabilistic analysis. Although most IaaS providers do not have access to the workloads being run by their customers, providers may monitor for anomalous usage patterns. After customers are up and running, account activity may, for example, be monitored by scanning metadata for indications of malicious activity as well as reviewing billing and payment history, service usage, and third-party abuse reports.

Companies may also use automated mechanisms to restrict potential malicious activity from customer accounts. For example, transmission control protocol port 25, an unsecured port for mail server use, enables the diffuse sharing of spam and malware. Infrastructure providers may block outbound port 25 access by default to prevent threat actors from sending spam, phishing emails, and malware. Likewise, companies may block connections to known command and control servers or rate limit or filter outbound requests to prevent them from being used for DDoS attacks.

Companies also described threat monitoring across their own infrastructure and services, as well as the dark web, to identify and flag suspicious behavior for investigation. Using both automated and human analyst-curated approaches, companies shared how they can identify various threat vectors and monitor for indications of malicious activity (e.g., phishing uniform resource locators, web shells, and cybercrime-as-a-service offerings). Existing trust groups and abuse reporting mechanisms that enable reports from other industry players, governments, or security researchers also play a role in enabling companies to identify and respond to abuse.

2.5. Responding to Abuse

If companies, including providers, detect unusual behavior or actual ADI, they may employ containment strategies to enable further examination and validation, which can include blocking suspicious accounts. If there are indications of potential abuse, companies typically conduct robust investigations and then take steps to mitigate it, such as disabling malicious domain infrastructure hosted on a cloud service. When confirmed abuse

[18] Credential stuffing is a type of cyberattack where credentials obtained from a data breach on one service are used to attempt to log in to another unrelated service, based on the premise that people often use the same credentials (e.g., user identification and password) across multiple accounts. See "Credential Stuffing," Crowdstrike, March 2022. What is Credential Stuffing? - CrowdStrike or "What is Credential Stuffing? Credential Stuffing vs. Brute Force Attack," accessed September 11, 2023. https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/

is associated with a particular account, companies can suspend accounts and block reuse of services. Companies typically take such steps on their own, without government involvement or legal process.

2.5.1. Mitigating Reseller Abuse

Mitigating abuse by resellers and their end user customers involves many of these same practices. As further outlined in Section 3, best practices for reseller management include allowing the resale of services only through authorized channels that may have additional terms and conditions and have undergone due diligence by providers. This includes customer identity verification as well as risk scoring based on specific pre-determined criteria. Providers themselves can play a critical role in mitigating the risk of security threats by proactively working with their resellers to drive a higher overall level of security hygiene. In addition, some briefers highlighted using enhanced account security features, such as security keys, multifactor authentication, identity protection, or digital passkeys, to increase friction for potential malicious actors that work to compromise reseller relationships. Providers also work with resellers to implement least privilege principles[19] and to reduce the overall number of reseller admins with privileged access. Finally, the prohibition of certain payment instruments, such as cryptocurrency, also limits abuse of both direct and reseller relationships.

Multiple company briefers identified variants of these practices and readily employ them to address threats to their infrastructure. Given these practices have direct applicability to combating ADI, there is an opportunity to associate their efficacy more directly with this specific threat and reinforce the need to employ them. Doing so could highlight them more broadly across the range of companies that are combating ADI. Options could include more formal vetting, streamlining, and alignment for broader consumption among the range of companies that combat abuse of their domestic infrastructure.

Despite these best efforts, sophisticated nation-state actors and cybercriminals still find ways to exploit domestic infrastructure to achieve their malicious goals. Additionally, the employment of the above techniques is not consistent across all IaaS providers. Small and mid-sized companies in the ecosystem are not likely to have access to the same resources and expertise to build and deploy capabilities and adopt best practices to combat ADI.

2.6. Role of Government

The U.S. government holds unique authorities not available to providers whose infrastructure is being abused, especially regarding the ability to disrupt threat actors at scale and bring them to justice. Several government agencies work both independently and collaboratively to monitor, detect, mitigate, and disrupt malicious cyber activity. These agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA), have distinct missions, objectives, and tools at

[19] Organizations that follow the least privilege principle can improve their security posture by significantly reducing their attack surface and risk of malware spread. See "What is the Principle of Least Privilege?" Palo Alto Networks, accessed September 11, 2023, https://www.paloaltonetworks.com/cyberpedia/what-is-the-principle-of-least-privilege; and "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." Ross, Ron et al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-171 Revision 2, February 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.

their disposal, based on each agency's statutory authorities. This may lend itself to overlapping and competing interests among the agencies, particularly in the case of addressing ADI.[20]

It is also worth noting that government has unique capabilities to work across the ecosystem to counter a particular threat actor. While companies may be well positioned to address ADI that traverses their networks, they may also be siloed with little or no understanding as to whether other providers see similar activity.

The National Cybersecurity Strategy states that the U.S. "will use all instruments of national power to disrupt and dismantle threat actors whose actions threaten its interests" by collectively integrating "diplomatic, information, military (both kinetic and cyber), financial, intelligence, and law enforcement capabilities" to incapacitate malicious actors' efforts to mount cyber-enabled campaigns.[21] This whole-of-government approach, utilizing various agency capabilities, is evident in recent disruption and take down campaigns.[22] That said, ADI poses unique challenges and opportunities to the U.S. government's ability to take appropriate action against malicious actors, as many of its current processes and tools cannot keep pace with the speed and scale of ADI.

For example, the operational methodology of ADI can be challenging to the FBI, which has historically prioritized reactive investigative efforts to support prosecutions rather than proactive disruption efforts. Procedures for the lawful pursuit of pertinent information or to obtain approval for disruptive actions, can take longer than the time scale in which these actors operate. Malicious actors can quickly "spin up" infrastructure and take it down, leaving only historical records of usage.

At the same time, in response to ADI, U.S. agencies have the ability to compel data through serving legal process on a provider that has a presence in the U.S., which may not be possible if the provider holding the data has no presence in the U.S.[23] Statutes that permit the government to compel data from electronic communications services and remote computing services that have a presence in the U.S., such as the Electronic Communications Privacy Act (ECPA, which includes the Wiretap Act),[24] and the Foreign Intelligence Surveillance Act.[25]

---

[20] For example, the Federal Bureau of Investigation (FBI) may prefer malicious actors to remain on domestic infrastructure so that they can use their tools to both monitor and disrupt those actors. On the other hand, the National Security Agency (NSA) may prefer that these actors operate on infrastructure outside of the U.S. so that they can leverage their intelligence gathering authorities.

[21] The White House, "National Cybersecurity Strategy."

[22] "Authorized Disruption of Snake Malware Network Controlled by Russia's Federal Security Service," U.S. Justice Department, press release, May 9, 2023, https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-snake-malware-network-controlled.

[23] Law enforcement briefers noted that the ability to compel evidence from U.S.-based providers is a significant benefit in obtaining timely data, as opposed to the data being located with an overseas provider.

[24] Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2523 (1986), Electronic Communications Privacy Act of 1986 (ECPA) | Bureau of Justice Assistance (ojp.gov).

[25] Foreign Intelligence Surveillance Act. 50 U.S.C. §§ 1805, 1842, 1861 (1978), National Security Agency/Central Security Service > Signals Intelligence > FISA (nsa.gov).

The intelligence community continues to play a key role in addressing malicious cyber activity. For example, the NSA – most recently through their Cybersecurity Collaboration Center (CCC) – often turns intelligence-derived insights into actionable indicators and relevant information for other government agencies, partners, and industry stakeholders. However, malicious cyber actors operating on U.S. domestic infrastructure complicates the ability of the NSA to provide intelligence-driven insights for cyber defenders, particularly given the attribution challenges noted in the Executive Summary on page ES-1.

Further complicating U.S. government efforts to address such abuse is the practice by some domestic infrastructure providers to use foreign resellers for their services. When this occurs, U.S. law enforcement agencies must seek the necessary information held by foreign providers with no presence in the U.S. through mutual legal assistance processes, such as a treaty or letters rogatory, and may not have jurisdiction to conduct disruptive actions. Processes to obtain information held by foreign firms through foreign governments can be lengthy – often exceeding the timeframe of malicious actors' operations, and negatively impacting its usability in investigations or other operations.[26] In some circumstances, the U.S. government may not have a viable method to seek assistance from the foreign country, in which case the evidence may be completely out of reach.

Multiple agency briefings identified in how industry can best assist the U.S. government in combatting ADI. Some U.S. government agencies spoke to the need for enhanced collaboration and additional information sharing; however, the specific information the government seeks from the private sector to address ADI remains unclear and could very well depend on its ultimate purpose. 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. In fact, one key government representative noted that relevant information is "situation-specific and circumstantial, and there is no one answer all of the time." Further, the intended purpose will also drive the timeliness with which such information is shared.

For example, some government briefers proposed suspicious activity reports (SARs) for cyber activity, similar to the SARs that the Bank Secrecy Act[27] requires financial institutions to file with the Financial Crimes Enforcement Network whenever there is a suspected case of money laundering or fraud. Certain indicators, such as cash transactions over $10,000 per day, trigger this reporting requirement for financial institutions. While the committee heard suggestions from government briefers that a similar mechanism could apply to hosting providers who observe suspicious activity by cyber actors, the committee did not hear what specific information would be sought, what activity would meet a threshold, and how this information could be useful in preventing or responding to ADI. Furthermore, it is not clear what resources would be required for private entities to report this

[26] Law enforcement characterized the "reseller problem" as a key challenge in combating ADI. Foreign-based resellers may purchase U.S. based services and offer them for resale, without undertaking efforts to mitigate abuse of these services in the same manner that the U.S.-based provider may undertake. Some resellers are specifically sought out by cyber criminals because they have fewer registration restrictions for new accounts and services and require minimal identity authentication.

[27] Bank Secrecy Act of 1970. 31 U.S.C. § 5311 *et seq*. (1970), The Bank Secrecy Act | FinCEN.gov.

activity, which U.S. government agencies would receive the information, and whether the government has the resources needed to collect and analyze these reports.

Moreover, the Bank Secrecy Act[28] includes a safe harbor for financial institutions that does not apply to information technology providers. Briefers to the committee also noted that SARs in the financial sector are one-way; information is shared with the government but not by the government to the private sector. Additionally, briefers noted that the financial sector is positioned very differently, in that its institutions can see the content of financial transactions, which makes these reports more useful, versus infrastructure providers who generally do not have access to customers' content. While there may be lessons learned from the model employed in the financial services sector that could be applied to infrastructure providers to help address abuse, there is not a direct parallel between the sectors and further analysis would be required to justify pursuing SARs for cyber activity.

While the U.S. government has a host of tools and capabilities it can bring to bear on malicious cyber activity, ADI poses unique challenges that require thorough consideration and analysis to determine how best to address gaps and shortfalls.

2.7. Collaboration and Information Sharing to Mitigate ADI

Partnership has long been a central tenet in efforts by the government and the private sector to address cyber threats. Briefers reinforced the importance of partnership and the resulting collaboration. While the U.S. government has some insight into various malicious activities through intelligence gathering or investigation, its perspective is limited based on its visibility and prioritization of resources. Technology companies, in turn, may have visibility into potential and existing malicious activity when the activity takes place with, on, or through systems and services those companies own, lease, and manage, but may not have insight on activity outside of their own systems. Collaboration across the public and private sectors could allow a more complete picture of ADI activity than any stakeholder could develop alone. As articulated by government briefers, the goal should be to build collaborative mechanisms and partnerships that enable security professionals to track and respond to threats as they arise, regardless of the infrastructure used.

There is an abundance of organized and informal efforts for collaboration. Collaboration mechanisms for addressing malicious cyber activities, which can include efforts to combat ADI, range from public exchanges of information through social media to informal, one-on-one personal relationships; to larger trust groups; to more formalized mechanisms. Some are government-sponsored, while others may reflect a collection of industry threat analysts from a single sector, or alternatively a diverse mix of industry, government, and civil society experts.

Collaboration to address malicious cyber activities could include a range of activities from operational actions to information sharing. Many ISPs routinely discover and disrupt the activities of malicious cyber actors, both when such actors target that provider's own infrastructure and when actors abuse or misuse those services to attack

[28] Ibid.

third parties. Episodes such as the Conficker worm in 2009, VPNfilter in 2018, or Emotet in 2021 underscore how collaboration to understand and takedown abusive actors is a constant effort in cyberspace.

Multiple briefers raised information sharing as a key aspect of mitigating ADI today and in the future. Companies throughout the supply chain have visibility into ADI when the associated malicious activity transpires with, on, or through systems and services those companies own, lease, and manage. As shown in the illustration in Section 1, this makes it incredibly difficult if not impossible for even the most sophisticated malicious actors to avoid generating data that can be analyzed to track and disrupt their operations.

Industry experts collaborate today to leverage their unique data holdings to track and disrupt malicious cyber activity, but these efforts can be relatively limited either in scope, scale, or focus. Various stakeholders routinely share malware samples through private and government channels to develop signatures and automated cleanup tools, identify exploitation of previously unknown vulnerabilities, and warn of evolving tradecraft. They also produce and share in-depth analysis of advanced malicious activity to enable detection, disruption, and remediation, as well as to improve defensive countermeasures. At scale, an entire commercial industry of cyber threat intelligence, powered by reverse engineers, linguists, and analysts, create actionable content that is consumed by defenders inside and outside government. Many analysts who work for these companies have established professional relationships and analytic partnerships with analysts at other companies that can exchange different perspectives on ADI. Often such analyses are made publicly available, allowing other companies to build on the work and track additional infrastructure belonging to the same actor(s).

However, briefers pointed out that for many companies, such collaboration is often viewed as an ancillary duty, with few formal resources or incentives available for sustained participation and an absence of a coherent strategy to combat ADI as a guide. While a variety of mechanisms already exist for collaboration, there is room for improvement and additional focus on ADI. More coordinated efforts across industry, particularly with respect to identifying ongoing ADI and identification of fraudulent accounts across providers and services, have the potential to add significant cost to and undermine the effectiveness of malicious activities. Briefers also suggested exploring mechanisms to better recognize, resource, and reward collaboration within government, within industry, and between the two.

2.8. Government-Established Public-Private Partnerships

Many past and ongoing initiatives have fostered collaboration to combine the capabilities and authorities possessed by different government actors and align them with industry capability and insights. Across government, these 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).

Within government, CISA plays a significant role in defending against ADI. As noted earlier, various providers have insight into the details of malicious cyber activity. These details, such as indicators of compromise, are crucial in preventing and mitigating future instances of malicious cyber activity. While the U.S. government has

some insight into various malicious activity through intelligence gathering or investigation, its perspective on ADI. is often limited.

CISA, through the JCDC, seeks to bring multiple providers together, along with relevant U.S. government agencies, to form a more complete picture of malicious activities that include ADI. Doing so enables defensive action by relevant stakeholders, which often includes both government agencies and private sector partners. JCDC works to disseminate threat information to potential targets, which is a key element in how JCDC can enable the better protection of domestic infrastructure. CISA shares threat intelligence, either specifically to affected or vulnerable companies, and more generally through threat alerts, which are often issued jointly with other U.S. government agencies (typically FBI and NSA) and even with other foreign governments. These alerts notify the private sector of potential or ongoing threats, and what companies can look for to protect themselves against the malicious activity. These efforts to assist defenders are important for combating malicious abuse because actors do not only abuse virtual resources hosted in the cloud, but also may obfuscate their campaign origins by commandeering on-premises systems.

Importantly, JCDC seeks to transform basic information sharing into more comprehensive operational collaboration, through which partners not only exchange actionable data but also carefully sequence their actions to execute joint defensive operations that impose lasting, strategic costs on malicious actors. In that way, JCDC presents opportunities to build on siloed anti-abuse programs to create a more holistic effort to disrupt malicious networks, and one of the committee recommendations looks to leverage this opportunity through a pilot project.

While the committee received limited input from the NSA, what the committee did find is that it can leverage its signals intelligence and cybersecurity operations across national security systems to generate unique insights into nation-state intentions and capabilities in cyberspace.[29] NSA analysts and private entities often collaborate through the CCC, which enables the NSA to scale "intelligence-driven cybersecurity" through its partnerships.[30] The NSA's Cybersecurity Directorate and the CCC share NSA's analysis and subject matter expertise on cyber actors and threats to empower the private sector to take action to mitigate cyber threats, including ADI. While their primary goal is protecting the defense industrial base, any such efforts to share cybersecurity information can then cascade to better protect any of the critical infrastructure sectors, consumers, and allies.

As is observed in many recently announced U.S. government cyber actions, success is built upon the collaboration and coordinated action of many different actors including international partners and the private

[29] "Cybersecurity 2022 Year in Review," National Security Agency (NSA), 2022. https://media.defense.gov/2022/Dec/15/2003133594/-1/-1/0/0139_CSD_YIR22_FINAL_LOWSIDE_ACCESSIBLE_FINAL_V2.PDF

[30] "NSA Cybersecurity Collaboration Center," NSA, accessed September 6, 2023. https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/

sector. This type of action can include joint cybersecurity advisories, or a multi-agency operational campaign.[31]

2.9. Industry Partnerships and Trust Groups

Collaboration is not limited to public-private partnerships. Industry partnerships exist as well, including formal organizations such as a variety of Information Sharing and Analysis Centers/Information Sharing Analysis Organizations, the Cyber Threat Alliance, the Anti-Phishing Working Group, and a much larger number of one-to-one relationships as well as informal, ad-hoc trust webs that include industry experts.

Trust groups comprise tight-knit sets of security professionals, typically sector specific, who voluntarily collaborate through private channels to contribute their knowledge and visibility—often provided via their full-time role working for a technology company or service provider—to track and disrupt malicious actors. Groups with diverse members hailing from various sectors can analyze data from multiple perspectives and form a high-fidelity view of malicious activities. Their informal structure allows them to avoid organizational interests that might hamper sharing (such as concerns by a given corporation about working with competitors) and convene quickly around specific threats to share relevant information quickly. Trust groups can play a constructive role in combating ADI.

Multiple briefers highlighted the work of trust groups in combating ADI, while noting their limitations, such as express legal authority to act. Even simple notifications to victims or providers whose services are being abused can expose well-meaning volunteers to potential legal action that chills proactive efforts to combat ADI. Likewise, trust group members who participate based on their industry roles may face corporate limitations on what they can do or share. For similar reasons, many trust groups are hesitant to call attention to their successes, making it difficult to leverage or assess their current impact.

Another limitation with trust groups is their small size and reliance on personal relationships, which limits their ability to grow and makes it difficult for new companies or new individuals without pre-existing trust relationships to break in and collaborate with a group. Trust groups can grow to a size in which members no longer trust the full membership, and then information sharing begins to erode. Additionally, members sharing restricted information (such as Traffic Light Protocol (TLP): Red[32]) outside of the group can quickly fracture and reduce trust, and the sharing of data against company policies or user agreements can have ramifications for their employment. Some individuals belong to multiple trust groups, which creates overlap between the groups and can complicate sharing restrictions. Finally, the volunteers who support these groups are not always resourced to

[31] In this 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, further highlighting the importance of partnerships across the U.S. government and internationally. "Joint Cybersecurity Advisory: Hunting Russian Intelligence 'Snake' Malware," CISA et al, May 9, 2023. https://www.cisa.gov/sites/default/files/2023-05/aa23-129a_snake_malware.pdf

[32] Traffic Light Protocol (TLP) is a simple color-based system for indicating with whom potentially sensitive information can be shared. See Traffic Light Protocol (TLP) Definitions and Usage | CISA or Traffic Light Protocol (TLP) (first.org)

support the efforts by their employers, depending on if the sharing groups are company-sanctioned or not, and do so at the expense of their personal time.

3. Key Issues

3.1. Legal Barriers

The committee found that certain actual or even perceived legal barriers may impede activities by infrastructure operators and government agents that could otherwise assist in preventing or disrupting abuse by malicious cyber actors. These barriers often occur when the action requires the exchange of information or other collaboration between or among participants in the ecosystem. And yet collaboration among infrastructure and communications service providers, network owners, cybersecurity technology vendors, and governmental entities is often essential because none of these ecosystem participants on their own has comprehensive visibility into the threat landscape or sovereignty over all relevant infrastructure.

A recurring theme in committee briefings was the inherently multijurisdictional nature of this complex ecosystem, and the reality that technology businesses operating in the U.S. must comply with an increasingly global set of legal requirements around the collection, use, retention, and destruction of the data they process or control. The resulting patchwork of governing statutes, regulations, and commercial agreements – and the uncertainty around which legal regime(s) may apply in certain circumstances – is seen as responsible for much of the friction in strategies to collaboratively address infrastructure abuse.

Stakeholders across the cybersecurity landscape share a perception that U.S. businesses will often hesitate to engage in multilateral actions because the indeterminate risk of potential legal liability and reputational harm tends to override the nebulous and indirect benefits for businesses. In general, there are fewer perceived or actual barriers to sharing information associated with a threat actor, but information about victims is more difficult to lawfully share without consent of the victim.[33]

For these private-sector entities, the assessment of legal constraints must account for the following sources of law, among others:

- **Contracts:** Technology firms are increasingly bound to comply with myriad customer and vendor requirements around data privacy and security incorporated into their commercial agreements. The

[33] This difficulty is not hypothetical or limited to the ADI context. By way of illustration, the Information and Communications Technology Supply Chain Risk Management Task Force, a Critical Infrastructure Partnership Advisory Council (CIPAC)-chartered public-private partnership co-chaired by CISA, the Information Technology Sector Coordinating Council, and the Communications Sector Coordinating Council, studied an analogous problem regarding the legal impediments companies face in sharing supply chain risk information regarding suppliers. Amongst other findings, the Task Force determined that CISA 2015's liability protections for sharing cyber threat indicators were insufficient to protect companies seeking to share supply chain risk information, because such information was not explicitly defined as a category of covered Cybersecurity Threat Indicators. See, "Working Group One: Extension Period Report, Preliminary Considerations of Paths to Enable Improved Multi-Directional Sharing of Supply Chain Risk Information," Communications Sector Coordinating Council (CSCC), Cybersecurity and Infrastructure Security Agency (CISA), and Information Technology Sector Coordinating Council (ITSCC), September 2021, https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force_multi-directional-sharing-scri_508.pdf; and "Information and Communications Technology Supply Chain Risk Management Task Force Year 2 Report, Status Update on Activities and Objectives of the Task Force," CSCC, CISA, and ITSCC, December 2020, https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force_year-two-report_508.pdf.

agreements – which may reflect standard corporate or industry policies but may also include bespoke terms – typically regulate where and how data is stored, who has access to it and by what means, the purposes for which it can be used, and with whom, and under what circumstances, it may be disclosed. In many cases, these contracts will include provisions requiring customer notification or consent for disclosure.

- **Government Regulations:** Depending upon the industry in which the business (or its customers) may operate, an assortment of regulatory requirements may attach to classes of data affected or targeted by malicious cyber activity. For example, customer proprietary network information, healthcare information, financial account information, government information, electronic communications content/metadata, and material non-public corporate information are all categories of sensitive data potentially covered by various distinct U.S. regulatory regimes.

- **Trade Restrictions:** Software code and other technologies, including malware and encryption technology, may be subject to legal constraints on cross-border transfers.

- **Privacy Laws:** Numerous jurisdictions (sometimes at both a national and state/provincial level) have adopted data privacy legal regimes that constrain how companies may collect, process, store, and transfer the personal data of their customers. These laws typically apply to information used to identify a specific person (e.g., name, address, date of birth, etc.) but also may apply to infrastructure-related identifiers, such as email addresses or even IP addresses, typically considered cyber threat indicators and often shared for threat detection. Among the most prominent of these privacy laws is the European Union's (EU) General Data Protection Regulation (GDPR), which applies globally to companies or organizations that offer goods or services to people within the EU and carries the threat of hefty fines (up to four percent of annual corporate revenue) for non-compliance.

Although there may be scenarios under which cyber threat information sharing would be permissible under these legal regimes, the lack of clarity and potential for penalties and reputational harm is a significant disincentive for companies to share information. Companies that do business with non-U.S. customers may adopt conservative legal positions on data sharing to remain competitive and reduce legal risk in certain markets. 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, EU data protection authorities issued a number of opinions scrutinizing the ability of companies processing the personal data of EU citizens to use U.S.-based cloud service providers consistent with GDPR due to concerns about U.S. government agencies' ability to access such data.[34] Those decisions put pressure on U.S. companies to justify their positions on data privacy. An increasing European focus on "sovereignty" requirements, such as proposed requirements in the European Cybersecurity Certification Scheme for Cloud

[34] See, for example, "2022 Coordinated Enforcement Action, Use of cloud-based services by the public sector," European Data Protection Board, adopted January 17, 2023, https://edpb.europa.eu/system/files/2023-01/edpb_20230118_cef_cloud-basedservices_publicsector_en.pdf

Services,[35] also affect companies' ability and legal certainty to share data. Some larger U.S. cloud companies have even announced partnerships with non-U.S. providers to comply with these "sovereignty" requirements for European countries,[36] which would restrict their own access to data, including threat information, for business purposes. Without more international collaboration and agreement about the importance of private sector entities both sharing and having access to threat indicators across borders, threat information is likely to become increasingly siloed and cyber defenders will be further inhibited.[37]

Meanwhile, the information flow from the government to the private sector is also subject to legal constraints. For U.S. government agencies, actual or perceived barriers to information sharing may include, among other things:

- the Privacy Act;[38]
- the Right to Financial Privacy Act;[39]
- laws requiring safeguarding of classified information or grand jury information; and
- administrative barriers for federal personnel to share detailed, actionable information with individuals who do not hold clearances.

The committee observed that there are existing and emerging legal protections and incentives – and even mandates – in some jurisdictions that successfully promote the sharing of threat intelligence between the private sector and the government. However, gaps remain. For example, Congress enacted the Cybersecurity Information Sharing Act of 2015 (CISA 2015[40]) for the express purpose of promoting the exchange of cyber threat indicators and defensive measures between and among public- and private-sector organizations. CISA 2015 permits most forms of sharing cyber threat indicators and defensive measures "notwithstanding any other provision of law" (for example, antitrust law or privacy/surveillance laws) when the exchange is conducted "for a cybersecurity purpose."[41] It also broadly shields private parties involved in the exchange of such information from civil or criminal liability by providing that "[n]o cause of action shall lie or be maintained in any court against

---

[35] These requirements would limit the highest level of certification to European Union (EU)-based legal entities or those "immune" from non-EU laws (including U.S. laws) to prevent access to data by non-EU countries.

[37] Peter Swire, DeBrae Kennedy-Mayo, and Drew Bagley, and Avani Modak, Sven Krasser, and Christoph Bausewein, Risks to Cybersecurity from Data Localization, Organized by Techniques, Tactics, and Procedures (June 1, 2023). Available at SSRN: https://ssrn.com/abstract=4466479 or http://dx.doi.org/10.2139/ssrn.4466479; Coalition to Reduce Cyber Risk, "Better Connected: How International Data Flows Enable Stronger Cybersecurity," Apr 24, 2023.

[38] Privacy Act of 1974, as amended, 5 U.S.C. § 552a (1974). https://www.justice.gov/opcl/privacy-act-1974

[39] Right to Financial Privacy Act, 12 U.S.C. Chapter 35 (1978). https://www.ecfr.gov/current/title-31/subtitle-A/part-14

[40] Cybersecurity Information Sharing Act of 2015, 6 U.S.C. § 1501-1510 (2015). https://law.justia.com/codes/us/2015/title-6/chapter-6/subchapter-i/

[41] 6 U.S.C. § 1503(c)

any private entity, and such action shall be promptly dismissed" for any otherwise-authorized sharing of cyber threat intelligence information.[42]

Despite these broad pronouncements, however, the liability safe harbor provided by CISA 2015[43] 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 GDPR.
- It only applies when information exchanges are "conducted in accordance with"[44] several specific technical requirements, including the advance removal of certain personal information, and use of a particular process within the Department of Homeland Security.[45]
- It does not sufficiently incentivize the sharing of other categories of information beyond cyber threat information that may be useful in the ADI context.
- The scope of its preemptive and liability-shield provisions has not been fully tested.

Therefore, while CISA 2015 encourages the sharing of a circumscribed set of cyber threat information, private entities remain uncertain about the legal risk of participating in some threat intelligence exchanges. Briefers also noted that relevant provisions of CISA 2015 are not well-understood by private industry outside of a relatively small universe of subject-matter experts.

Additionally, a company may also be reluctant to proactively identify malicious activity on its platform, as it could create risk, including increased liability. If the company takes action to disrupt abuse, but in the process reveals a previously unrecognized problem, it may trigger unwelcome scrutiny (or even legal claims) from customers, regulators, the media, or others. If, on the other hand, it takes no action, the abuse will continue, and the company may incur a risk of liability to third parties from inaction. This dilemma, some experts suggested, disincentivizes some companies, particularly smaller providers, from conducting threat-hunting operations on their networks and services.

The committee also noted that there are limited legal protections available to infrastructure operators who act based on "false positives" and thereby disrupt legitimate use that is mistakenly identified as abuse. Malicious actors go to great lengths to hide inside the noise of benign user traffic, and so identifying abusive activities is often based on probabilistic judgments that are well short of certainty. An erroneous disruptive action, however,

[42] 6 U.S.C. § 1505(b)

[43] 6 U.S.C. § 1503-1505

[44] Ibid

[45] 6 U.S.C. § 1503-1504

could cause serious harm to innocent customers, leading to loss of business, harm to business reputation, or even civil damages.

3.2. Resource Gaps

Detecting cyberthreats is an arduous task. Providers looking to detect similar threats across their services often need to detect anomalies at scale, potentially across millions of accounts. In practice, that means deploying tools that can help identify suspicious activity and, when possible, automatically mitigate it. Because those services may not always be commercially available, companies may have to build their own tools.

At the level of an individual organization, both government agencies and companies employ threat detection tools that analyze user behaviors. These tools are especially effective with a model like zero trust where users require frequent authorization. They also can help organizations combat ADI, such as by mitigating the impact of malware, protecting against ransomware and identity theft, and improving endpoint security. With the help of effective threat detection mechanisms, applications and data can be protected against sophisticated cyber-attacks. While current detection tools are readily available for the type of attacks that occur today, future attacks will be more advanced. This necessitates government and private industry investment in R&D for the design of more advanced tools and methods to detect cyber threats.

In addition, entities of various sizes have access to different resources. Small and mid-size infrastructure providers don't always have protections against common forms of abuse (like tools to prevent account compromise or even fraud), because of (1) cost; and (2) lack of a shared understanding about what kinds of protections/tools could effectively prevent abuse. There is an opportunity both to level set on government expectations for providers, identify what kinds of tools providers should have, and to help small and mid-size providers get access to them.

3.3. Improving Security in the Reseller Ecosystem

As noted in Sections 1 and 2, IaaS providers and other relevant companies such as virtual hosting providers and DNS registrars can sell services either directly or through intermediaries, known as resellers. These resellers enter into agreements with providers that enable them to resell information technology services to their customers, sometimes packaged by resellers with other specialized services such as strategy and migration services, systems integration, managed security and compliance services, or other consulting services. Reseller account volume is a tiny percentage of total sales and foreign resellers comprise an even smaller percentage.

Although they are a legitimate and valuable element of the global cloud business ecosystem, some briefers stated that resellers and managed service providers have emerged as a target for threat actors and a vector for IaaS abuse. Malicious actors target resellers and managed service providers because, as one briefer explained, their security controls and practices may be weaker than those of the hosting providers whose services they are reselling (e.g., weak/default passwords, inactive multi-factor authentication, poor patch management). Resellers may have more technical data on their customers than the underlying provider and some level of access to their accounts. Further, one reseller might manage dozens of customers, meaning that a single compromised reseller

administrator account could grant malicious actors access to potentially many more user accounts from which to launch attacks.

Hosting providers themselves can play a critical role in mitigating the risk of security threats by proactively working with their resellers to drive a higher overall level of security hygiene. Several security best practices can be employed that serve to enhance the security of reseller relationships. Hosting providers may:

- Require all privileged account holders, such as reseller administrators, to receive regular security awareness training.
- Provide reseller administrators with enhanced account security features, such as security keys or digital passkeys, and enforce multi-factor authentication on high-risk accounts by default.
- Work with resellers to implement least privilege principles and to reduce the overall number of reseller administrators with unnecessary access.
- Prevent resellers from accepting certain forms of payment from customers that could be problematic, such as crypto currency.

These measures may not eliminate the risks of abuse associated with compromised resellers, but they can play a significant role in reducing the attack surface and raising the costs associated with ADI.

3.4. KYC Requirements

3.4.1. Overview

One of the solutions that has been discussed to address ADI by malicious foreign actors is to institute KYC requirements on U.S. infrastructure providers through identity verification schemes modeled after those employed in the financial sector. This approach was most notably set forth in EO 13984 issued on January 19, 2021, titled, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities."[46] This EO requires the Department of Commerce to issue regulations mandating U.S. IaaS providers verify the identity of a foreign person that obtains an account, including "securely maintaining" a foreign customer's national identification information.

The EOP requested that the committee explore the state of that implementation effort and its potential relevance to addressing ADI. Given rulemaking pursuant to the EO has been under consideration by the U.S. government concurrent with this study, many briefers representing public and private sector organizations opined on the efficacy and utility of this approach, with mixed views. Some representatives in the U.S. government suggested that KYC would provide greater ecosystem transparency and improve threat monitoring, such as through standardizing data collection. However, at least one U.S. government representative acknowledged that KYC does not support a collaborative approach to addressing ADI, highlighting that information that would provide value to addressing ADI is situationally specific and will vary based on the circumstances. Instead, KYC

[46] The White House, Executive Order No. 13984, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities."

information assumes a certain common value of specific pieces of information (i.e., national identification number). This briefer also noted that they do not have any data about whether such a requirement would be useful, and said that malicious actors often change their tactics, techniques, and practices in response to new regulatory requirements. Private sector representatives highlighted the lack of alignment between the proposed IaaS and existing financial services KYC models, the unproven ability of KYC to prevent ADI or facilitate post-attack forensics, and the potential for unintended consequences, particularly with respect to privacy and U.S. competitiveness in the global market.

3.4.2. Financial Services Model

Some briefers shared the perspective that the use of KYC measures in the financial sector can be used as a model for the IaaS industry. They highlighted attributes that are perceived to be analogous between the financial sector and IaaS sector, even though some financial sector representatives considered their version of KYC to be of limited utility. Other experts indicated that there are several differences between the financial sector and IaaS providers that regulators should be aware of in pursuing any such effort. A key distinction noted is the velocity difference for signing up for a bank account, as opposed to signing up for a cloud services account (and the rapid change expected by the introduction of new services). The committee was unable to obtain any data or study to support a comparative analysis.

3.4.3. Efficacy of KYC

Some briefers cautioned against implementing KYC requirements, noting that KYC efforts, particularly those targeted at "foreign persons," are unlikely to be effective in addressing the actual threat. Briefers highlighted that the actors U.S. investigators are most concerned with (such as nation-state-backed advanced persistent threat actors) are also those that are most likely to successfully use sophisticated methods to bypass such requirements by appearing to be U.S. persons or alternatively, use other means such as compromising infrastructure to conduct malicious activity. This could be accomplished through means including the use of compromised U.S.-based IP addresses, via VPN services, U.S.-based VOIP, or U.S.-based physical address and phone numbers. Multiple briefers noted that KYC rules and regulations would likely do more harm than good if implemented to protect against cybersecurity threats. More specifically, a potential repercussion of KYC rules is that the identity-fraud market would expand to meet attackers' demand for seemingly legitimate user credentials and accounts. Thus, additional exposure of users' personally identifiable information would occur during infrastructure breaches.

Multiple briefers also raised the concern that malicious actors may move their operations to non-cooperative virtual infrastructure providers located outside the U.S. to circumvent KYC requirements. This outcome would limit the potential for voluntary action by providers and pose different challenges and opportunities for various U.S. government stakeholders, depending on whether the agency is dependent on using domestic legal process

and authorities, or whether the agency is foreign focused in its data collection, such as those activities set forth in Executive Order 12333 on United States Intelligence Activities.[47]

Moreover, briefers noted the KYC requirements under discussion do not clearly address the issue of resellers noted above as it is often a customer of a foreign reseller that is engaged in abuse, rather than an individual purchasing services directly from the IaaS provider who would actually be within the scope of a U.S. regulation. Finally, at least one briefer noted there could be a chilling effect on legitimate use of U.S. infrastructure by foreigners operating under authoritarian foreign regimes who may be reluctant to provide KYC data for fear the information may become known to their domestic security apparatus and open them up to government reprisals.

3.4.4. Privacy Implications

Several briefers raised the potential for serious privacy implications in collecting and retaining additional personal identification information, both domestically and internationally. One briefer explained specific challenges with regard to U.S. allies taking issue with U.S. laws and policies that target foreign persons or data. For example, the European Commission (EC), and officials from EU member states have raised persistent and widespread objection to the Clarifying Lawful Overseas Use of Data Act (CLOUD Act),[48] which was passed in 2018 and clarified that in response to legal process, U.S.-based providers must produce data in their possession, custody, and control even if the data is located outside the U.S.

In another example that was raised, the U.S. and EC recently negotiated a new Transatlantic Data Privacy Framework to enable transatlantic data flows after the Court of Justice of the European Union invalidated the prior Privacy Shield framework in the *Schrems II*[49] decision, finding that U.S. foreign intelligence surveillance authorities and practices did not meet the requirements of EU law. In July 2023 the EC adopted an adequacy decision to implement the new Data Privacy Framework, following U.S. implementation of its key commitments pursuant to EO 14086, Enhancing Safeguards for United States Signals Intelligence Activities,[50] which included publication by the Office of the Director of National Intelligence (ODNI) of updated policies and procedures covering all 18 intelligence community elements to implement enhanced privacy and civil liberties safeguards.

The U.S. government's willingness to update its intelligence community policies and procedures to strengthen the privacy and security protections is an acknowledgement of the importance of this issue. However, briefers noted that KYC requirements in EO 13984[51] could be viewed as a new U.S. surveillance initiative which

---

[47] Executive Order 12333, "United States Intelligence Activities," The White House, December 4, 1981, National Security Agency/Central Security Service > Signals Intelligence > EO 12333 (nsa.gov).

[48] "ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence," European Data Protection Board, (undated), https://edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf

[49] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559 (July 16, 2020).

[50] Executive Order No. 14086. "Enhancing Safeguards for United States Signals Intelligence Activities," The White House, 87 FR 62283 October 7, 2022, Federal Register: Enhancing Safeguards for United States Signals Intelligence Activities.

[51] The White House, Executive Order No. 13984, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber- Enabled Activities."

discriminates against EU persons and could create enormous doubt about the good faith of the U.S. government on surveillance policies. Briefers thought this impression would threaten not only U.S. competitiveness abroad, but it would also threaten U.S.-EU relations at a time when transatlantic solidarity is critical to preserving the open internet and the rules-based order.

In response to questions about privacy concerns from KYC obligations, one U.S. government briefer noted that banks have protected "safe harbor" reporting requirements that are built into the KYC rules to protect financial institutions and their members. For example, certain data collection can only happen once suspicious activity is confirmed to have occurred or be occurring. One briefer noted that overseas customers have not raised concerns because international banks must abide by similar regulations outside the U.S., especially in Europe; however, there is not a comparable KYC regime outside of the U.S. for internet ecosystem companies.

3.4.5. Inhibiting Competitiveness

Briefers also highlighted that privacy concerns may ignite or exacerbate digital protectionist initiatives, including increased sovereignty efforts in the EU, and drive customers away from U.S. IaaS providers. This is a concern for U.S. companies, and it should also be a concern for the U.S. government in light of global technology competition, as well as the benefits of having providers that share the U.S. government's objectives on combatting ADI. There is concern that the prime beneficiaries of U.S. KYC requirements will be Chinese cloud providers like Alibaba and Huawei, especially in those emerging markets where concerns about Chinese data collection are not a priority, and where Chinese companies are already engaged in aggressive campaigns to outcompete their U.S. rivals and broaden China's technological sphere of influence.

In addition to these concerns, the impacts of KYC are likely to be felt differently based on company size and scale. One briefer noted the significant business impact KYC requirements imposed by another government had on their operations in that jurisdiction because customers did not want to provide requested additional information. Another briefer also noted the resource burdens for small and mid-size companies to take on the data collection/retention requirements.

4. Recommendations

Over the course of outlining the overall challenges associated with ADI, the NSTAC identified six actionable recommendations.

1. The NSTAC recommends that the president direct the Office of the National Cyber Director (ONCD) develop a multi-faceted strategy for combating ADI. The strategy and any recommended actions should be informed and prioritized as a result of a rigorous, data-centric understanding of the scale and extent to which malicious actors are abusing U.S. domestic infrastructure, as well as a review of national-level intelligence collection requirements for sufficiency and completeness with respect to ADI. The likely effectiveness of the recommended actions should also be considered. In addition, the NSTAC recommends, as part of this strategy, that ONCD create an interagency governance mechanism that will enable relevant agencies to coordinate in setting specific goals and objectives; prioritizing efforts and related trade-offs; and engaging and collaborating with stakeholders.

2. The U.S. government, working through CISA's JCDC and the NSA's CCC, should create an operational working group that includes relevant private sector providers and key government representatives to focus on enhancing tactical collaboration to address ADI. This working group should (at the classified level as necessary), analyze cases of ADI in real-time, identify malicious actors who are compromising multiple systems, determine what information can be shared on the actor/event, identify impediments to further collaboration, identify opportunities for joint responsive action, and determine whether joint responsive action should be taken.

3. Pursuant to the National Strategy to Advance Privacy Preserving Data Sharing and Analytics,[52] the U.S. government should, through the National Institute of Standards and Technology and other departments/agencies as appropriate, conduct a public-private pilot program to test the practical application of privacy enhancing technologies (PETs) to accelerate the development of at-scale data analysis of threats to domestic infrastructure. This pilot program should develop a proof of concept to evaluate the potential use of PETs, such as federated learning and differential privacy, to disassociate data from its source for analysis and sharing, enabling providers or the government to share aspects of information related to ADI even when sensitive data cannot be shared directly. This recommendation could also support the implementation of the operational working group described in the second recommendation.

4. The U.S. government should create a public-private task force to develop a framework that outlines best practices to mitigate ADI, including for managing reseller relationships. As noted in Section 2 of this report, several technology providers already conduct extensive counter-abuse measures that can be considered best practices to mitigate abuse while ensuring a focus on appropriate privacy protections. These best practices should be evaluated by the task force with the goal of formally identifying current best practices that the U.S.

[52] "National Strategy to Advance Privacy-Preserving Data Sharing and Analytics," National Science and Technology Council, The White House, March 2023, https://www.nitrd.gov/pubs/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf.

government can recommend for use, as well as developing a plan to review and update the practices over time. This framework could serve as the basis for the Commerce Department's implementation of Section 1(c) of Executive Order (EO) 13984, which allows for the Commerce Department to exempt IaaS providers from the Section 1(a) identity verification requirements.[53] The task force should also consider resourcing mechanisms that will support the adoption of best practices among small/medium service providers. This should be done and assessed before the Commerce Department promulgates data collection and retention requirements pursuant to EO 13984.[54]

5. The U.S. government, working through CISA, the NSA, the FBI, and the Department of State, should develop a strategy to share intelligence with international partners regarding U.S. government concerns about abuse of virtual resources, encourage joint operations, and facilitate collective defense. The strategy should enable the sharing of cyber information among governments and industry across borders to effectively address malicious cyber actors. The strategy should include evaluation of the recommended steps those partners take to deter, investigate, and respond to ADI in their own countries for their applicability to combatting ADI in the U.S. In addition, the U.S. government should conduct a review of international laws that may prohibit companies from proactively sharing information and identify possible remedies to address any issues identified.

6. The U.S. government, working through CISA and the Department of Justice (DOJ), should work with the appropriate entities through the Critical Infrastructure Partnership Advisory Council to coordinate the development of a set of recommendations with the private sector to update and enhance CISA 2015, which is set to expire on September 30, 2025. These recommendations should consider (1) clarifying current protections for those who share cyber threat information; (2) enhancing protections to include operational dialogue necessary for disruption coordination; (3) expanding the definition of cyber threat indicator or creating an additional category of shared information that qualifies for the liability safe harbor to explicitly include information about ADI victims; and (4) any other protections to encourage more private sector information sharing. CISA and DOJ should also make a significant effort in promoting the protections afforded by the updated version of CISA 2015 for public awareness.

---

[53] The EO provides the Commerce Department discretion to establish the requirements for an exemption, and the exemption requirements "may include a finding that a provider complies with security best practices to otherwise deter abuse of IaaS products." Ideally, the promulgation of these best practices and the ability to receive exemptions from the Know Your Customer (KYC) verification requirements could incentivize uptake of broader security measures that will be more effective at countering ADI.

[54] The White House, Executive Order No. 13984, "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber- Enabled Activities."

Appendix A. Scoping Paper

PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

Proposed Study: *Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors*

INTRODUCTION

Established in 1982, the President's National Security Telecommunications Advisory Committee (NSTAC) is an industry advisory body that provides the President with advice on information assurance, cybersecurity, and the information and communications technology ecosystem with respect to national security and emergency preparedness (NS/EP) concerns. The administration may task the NSTAC to conduct a new study, "*Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors*", to commence in 2023.

BACKGROUND AND PROPOSED SCOPE OF STUDY

Cyber operations are conducted through the Internet. Most cyber actors route their malicious activity through one or more intermediate systems before connecting to a victim's system to disguise the source of the activity and make it more difficult to track. These intermediate systems can be any system that is connected to the Internet, including compromised machines of other victims.

Malicious actors located overseas, however, are frequently using U.S.-hosted leased infrastructure—including Infrastructure as a Service (IaaS) and Platform as a Service products—as intermediate systems to target U.S. victims. IaaS offerings, like Virtual Private Servers (VPS), are a particularly common use case, with malicious actors often leveraging VPS computing power from domestic infrastructure providers to conduct malicious cyber activities. While the quality of service of U.S. infrastructure providers is one contributor, foreign actors are also likely incentivized by the protections afforded by U.S. laws, which together constrain the U.S. government's ability to take preventative actions independently or through a legal directive to private sector companies. Often, the speed at which U.S. authorities may act through compulsory legal processes is much slower than the speed at which an actor is able to establish, use, and abandon virtual infrastructure.

Enabling the public and private sectors to prevent cyber actors from abusing U.S.-based infrastructure is critical to defending NS/EP equities and other critical infrastructures. This study will investigate what voluntary actions Internet ecosystem companies are currently taking to prevent or mitigate the abuse of domestic infrastructure by malicious foreign actors and recommend how the government can incentivize additional action.[1]

To inform the recommendations, the study will investigate any existing barriers–including financial, legal, or privacy–that may be preventing Internet ecosystem companies from more systematically addressing malicious actors' abuse of their technology and services. The

[1] In this context, Internet ecosystem companies refers to least: Internet service providers, telecommunications providers, cloud and VPS providers, operating system developers, content delivery networks, Domain Name System service providers, cybersecurity companies, hosting providers, domain registrars, and Internet technology platforms.

1

PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

Proposed Study: *Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors*

NSTAC will also make strategic recommendations for how the U.S. government can address these barriers to incentivize disruptive actions (e.g., infrastructure takedowns) while maintaining a voluntary, private sector-driven operational model.

KEY QUESTIONS TO CONSIDER

Scope of Challenge:

At what scale are foreign adversaries abusing domestic leased infrastructure to conduct cyber-attacks? Does the foreign use of U.S.-hosted leased infrastructure constitute a significant NS/EP threat to the United States?

Operational Collaboration Models:

- How can U.S. public and private sectors more effectively partner to disrupt adversary abuse of domestic infrastructure? What coordinated operational actions would be most impactful in sustainably disrupting adversary operations?
- What types of mechanisms currently exist to facilitate data sharing about infrastructure abuse between Internet ecosystem entities?
- What type of data is most relevant to informing disruptive actions? What types of Internet ecosystem entities have visibility of that data and what can they lawfully share?
- How could expanded sharing and operational collaboration affect cross-border data flow agreements between the United States and its allies?
- The Commerce Department is currently implementing know-your-customer provisions as part of Executive Order 13984, *Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities*. What is the state of that implementation effort and what is its potential relevance to addressing domestic infrastructure abuse? Will this rulemaking address the challenge of multiple layers of foreign re-sellers?
- What barriers currently exist that make it difficult to identify and take disruptive action against foreign actors leveraging domestic infrastructure for malicious cyber activities?
- How do current U.S. laws affect the types of action that Internet ecosystem entities can take to address abuse of their infrastructure and services?

2

Appendix B. Summary of Key Elements of the Internet Ecosystem

Content Delivery Networks (CDNs): Content Delivery Networks, like Akamai and Cloudflare, own geographically distributed servers that cache and serve content quickly to end users in close proximity to those servers. Consumers of CDN services configure their networks so that end users connect through the CDN's network rather than directly to the hosting provider in order to improve website performance and reliability and protect the origin hosting server from certain kinds of cyberattacks. A user in India seeking to access a British news article served from a CDN, for example, could be served a cached copy of the article from a geographically proximate server in India, rather than having to reach the same content at the website host, which might be located halfway around the world. Because of this technical configuration, CDNs have access to IP addresses and other metadata about visitors to websites using their services. The majority of global web traffic is served through CDNs.

Domain Name System (DNS): Threat actors often use unique domain names to facilitate network communications between different virtual resources, including to lure victims or exfiltrate data. Unlike Internet Protocol (IP) addresses, whose use is often dynamic in nature, changing over intervals of time, domain name registration is often more persistent. The DNS system allows Internet users to find websites online by translating domain names into IP addresses. DNS services are provided by different types of providers, each of which has different visibility.[55]

DNS Registrars: Domain name registrars like GoDaddy and Tucows sell domain names. Like other virtual resources, domain names can be registered by malicious actors through a domain name registrar either in the U.S. or abroad as part of carrying out attacks against U.S.-based targets. Bound by contractual obligations to the Internet Corporation for Assigned Names and Numbers (ICANN), the nonprofit organization that oversees the assignment of domain names and IP addresses, registrars are required to collect certain data about ownership from those who register domain names. In recent years, in order to comply with foreign privacy laws like General Data Protection Regulation, domain name registrars have reduced the information about domain name registration data that is publicly available. This has impacted the ability to determine whether a domain name used for malicious activities is correlated with other domain names, making it more challenging to identify the full breadth of threat actor infrastructure.

DNS Registries: Domain name registries like Verisign or the Public Interest Registry manage top level domains like ".com" and ".org." Consistent with contractual ICANN obligations, they maintain the records of which

[55] The global domain name system (DNS) centralized root is managed by the non-profit Internet Corporation for Assigned Names and Numbers (ICANN) and governed through a multistakeholder model. The root is comprised of generic top level domain names (gTLDs) and country code top level domain names (ccTLDs). ICANN has contracts in place with domain name registries (e.g., Verisign, which runs .COM, or Public Interest Registry, which runs .ORG), which manage generic top-level domains (gTLDs) (e.g., legacy gTLDs like .COM, .ORG, .NET, .DNS and new gTLDs like .MOBILE, .ZIP, .APP) as well as registrars (e.g., GoDaddy or Namecheap) which sell second level domain names to consumers. Unlike gTLDs, for which ICANN sets the rules, individual countries or their designees determine how their own ccTLDs (e.g., .US, .CA, .TK) are run as well as the rules for registration.

individual domains belong to which people and organizations and provide information about the location of domain names throughout the Internet.

Hosting Providers: Hosting providers operate physical servers, and physical and virtual networks in the U.S. and abroad, which they may sell commercially as Infrastructure-as-a-Service (IaaS) to both foreign and domestic consumers. IaaS provides scalable computing power and endless virtual server capacity to anyone with an internet connection. This infrastructure can be sold directly by hosting providers, or sold indirectly through resellers or managed service providers, which might be located outside the U.S. The size of hosting providers can vary significantly, ranging from large providers – such as Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft (Azure), or Oracle Cloud Infrastructure (OCI) – to small and medium enterprises (SMEs), such as GoDaddy and RackSpace. Hosting providers are generally subject to national, regional, or local laws and regulations, along with contractual commitments to their customers.

IaaS services can be sold directly to the customer by the IaaS provider, or through intermediaries called value-added resellers. Resellers enter into agreements with providers that enable them to resell cloud infrastructure to their customers, often packaged by the reseller with specialized services including strategy and migration services, systems integration, managed security and compliance services, or other consulting services. Responsible providers often have well-established programs that levy specific, and sometimes rigorous, requirements on resellers. Although a legitimate and valuable element of the global cloud business ecosystem, resellers and managed service providers can be a target for threat actors and a vector for IaaS abuse. Depending on the terms of service and the reseller program requirements, government efforts to obtain information on customers of a reseller can prove to be challenging, as they may not collect or retain identification or payment information.

Internet Service Providers (ISPs): Internet Service Providers operate and often own the physical networks responsible for connecting computers across the globe. They run the core routers, participate in internet exchanges, and build and manage the actual cables in and among cities, states, regions, and countries. These vendors – such as AT&T, Comcast, Cox, Lumen, T-Mobile, and Verizon – sell services to individual consumers and businesses. Such entities are governed by telecommunications laws and regulations at the national, regional, or local levels.

Security Providers: Commercial security providers serve as an important component of the Internet ecosystem, developing commercial threat intelligence feeds, and helping businesses improve visibility and control over potential vulnerabilities in their networks, filter known threats, and deploy access restrictions and other security measures. Endpoint security providers can monitor devices for vulnerabilities, misconfigurations, and threats. Network security providers can enforce access restrictions, including through DNS or URL-based filtering, inspect traffic for threats, and segment networks. Identity providers can help securely authenticate the identity of users. All of these security providers can log activity, providing invaluable information in the event of a security incident.

Virtual Private Networks (VPNs) and proxies: VPNs and other forward proxies (including residential proxies) route user traffic through encrypted tunnels to remote servers owned by the VPN provider or others before sending the traffic on to its destination. This technical configuration is often used to mask the original user's IP address or

make it appear as though a user has connected to the internet through a location different than the user's actual location.

Appendix C. Membership and Participants

Table 1: Subcommittee Leadership

Name	Organization	Role
Mr. Stephen Schmidt	Amazon	Subcommittee Co-Chair
Mr. Hock Tan	Broadcom, Inc.	Subcommittee Co-Chair
Mr. Robert Hoffman	Broadcom, Inc.	Working Group Co-Lead
Mr. Sunjeet Randhawa	Broadcom. Inc.	Working Group Co-Lead
Ms. Jordana Siegel	Amazon Web Services (AWS), Inc.	Working Group Co-Lead

Table 2: Subcommittee Membership

Name	Organization
Mr. Chris Anderson	Lumen Technologies, Inc.
Mr. Drew Bagley	Crowdstrike Holdings, Inc.
Ms. Lily Beres	NightDragon Management Company
Mr. Christopher Boyer	AT&T Communications
Mr. Jamie Brown	Tenable Network Security, Inc.
Mr. Matt Carothers	Cox Communications
Ms. Kathryn Condello	Lumen Technologies, Inc.
Mr. Chris Cornillie	Google, LLC
Ms. Cheryl Davis	Oracle Corp.
Mr. Ray DeMeo	Virsec Systems, Inc.
Mr. David Forscey	Cybersecurity and Infrastructure Security Agency (CISA)
Ms. Katherine Gronberg	NightDragon Management Company
Mr. Brian Hendricks	Nokia Corp.
Ms. Anitha Ibrahim	AWS, Inc.

Name	Organization
Ms. Stephanie Kiel	Google
Mr. Kent Landfield	Trellix
Mr. Seth McKinnis	CISA
Mr. John Miller	Information Technology Industry Council
Ms. Jen Miller-Osborn	Palo Alto Networks, Inc.
Mr. Sean Morgan	Palo Alto Networks, Inc.
Mr. Richard Mosley	AT&T Communications
Mr. Steven Nelson	Goldman Sachs & Co, LLC
Mr. John O'Keefe	Broadcom, Inc.
Mr. David Oxley	AWS, Inc.
Ms. Jennifer Raiford	Unisys Corp.
Mr. Kevin Reifsteck	Microsoft Corp.
Mr. Mark Ryland	AWS, Inc.
Ms. Alyssa Starzak	Cloudflare, Inc.
Ms. Stephanie Travers	Lumen Technologies, Inc.
Mr. Eric Wenger	Cisco Systems, Inc.

Table 3: Briefers, Subject-Matter Experts

Name	Organization
Dr. Manos Antonakakis	Georgia Institute of Technology and Voreas Laboratories Inc.
Mr. Drew Bagley	Crowdstrike Holdings, Inc.
Mr. Leonard Bailey	Department of Justice (DOJ)
Mr. Paul Benda	American Bankers Association (ABA)
Mr. Richard Boscovich	Microsoft Corp.

Name	Organization
Mr. Christopher Boyer	AT&T Communications
Mr. Sean Boyle	Federal Bureau of Investigation (FBI)
Ms. Zoë Brammer	Institute for Security and Technology
Mr. John Carlson	ABA
Mr. Brian Carter	Chainalysis Inc.
Mr. Chris Compton	Microsoft Corp.
Mr. John Costello	Center for Strategic and International Studies
Mr. Kyle Creyts	Coinbase Global, Inc.
Mr. Silas Cutler	Institute for Security and Technology
Mr. Michael Daniel	Cyber Threat Alliance
Mr. Sean Evans	Department of the Treasury
Mr. Patrick Flynn	Trellix
Mr. John Fokker	Trellix
Mr. David Forscey	CISA
Mr. David Fosth	Microsoft Corp.
Mr. Michael Garcia	CISA
Ms. Aadil Ginwala	Bureau of Industry and Security, Department of Commerce
Mr. David Gucker	The Constant Company, LLC
Mr. Juan Hardoy	Microsoft Corp.
Mr. Trevor Hilligoss	SpyCloud, Inc.
Ms. Aurora Johnson	CISA
Mr. Steve Kelly	National Security Council
Ms. Riley Kilmur	Spur Intelligence Corp.

Name	Organization
Ms. Casey Knerr	MITRE
Ms. Jaqueline Koven	Chainalysis Inc.
Mr. Jason Lyons	Microsoft Corp.
Ms. Kristen Lane	FBI
Ms. Christine Lazcano	CISA
Ms. Naomi Lefkovitz	National Institute of Standards and Technology
Mr. Jason Leong	FBI
Ms. Reg Levy	Tucows, Inc.
Ms. Jen Miller-Osborn	Palo Alto Networks, Inc.
Russ McRee	Google, LLC
Ms. Katherine Moy	DOJ
Mr. Wolfgang Moser	FBI
Mr. Steve Nelson	Goldman Sachs & Co, LLC
Mr. David Oxley	AWS, Inc.
Mr. James Perry	Crowdstrike Holdings, Inc.
Mr. Chris Porter	Google, LLC
Mr. Mike Purtill	Office of the Director of National Intelligence
Ms. Kimberly Raleigh	DOJ
Mr. Brian Rexroad	AT&T, Inc.
Mr. Marc Rogers	Ransomware Task Force, and the CTI League
Mr. Mark Ryland	AWS, Inc.
Mr. Robert Sheldon	Crowdstrike Holdings, Inc.
Mr. Steve Silberstein	The Financial Services Information Sharing and Analysis Center (FS-ISAC)

Name	Organization
Ms. Jordana Siegel	AWS, Inc.
Ms. Alissa Starzak	Cloudflare
Mr. David Stern	CISA
Ms. Elke Sobieraj	National Security Council
Ms. Megan Stifel	Institute for Security and Technology
Mr. Kevin Stine	NIST
Mr. Vikram Thakur	Broadcom, Inc.
Ms. Bridgette Walsh	FS-ISAC
Ms. Alison Zitron	DOJ

Table 4: Subcommittee Management

Name	Organization
Ms. DeShelle Cleghorn	President's National Security Telecommunications Advisory Committee (NSTAC) Alternate Designated Federal Officer (ADFO)
Ms. Laura Penn	Edgesource Corp.
Mr. Barry Skidmore	NSTAC ADFO
Ms. Jennifer Topps	TekSynap Corp.
Mr. Carlus Townsend	Edgesource Corp.
Mr. Joel Vaughn	TekSynap Corp.

Appendix D. Acronyms

Table 5: Acronyms

Acronym	Definition
ADI	Abuse of Domestic Infrastructure
CCC	Cybersecurity Collaboration Center
C&C	Command and Control
CIPAC	Critical Infrastructure Partnership Advisory Council
CISA	Cybersecurity and Infrastructure Security Agency
DOJ	Department of Justice
DoS	Denial of Service
DNS	Domain Name System
EO	Executive Order
EOP	Executive Office of the President
FBI	Federal Bureau of Investigation
GDPR	General Data Protection Regulation
IaaS	Infrastructure as a Service
ICANN	Internet Corporation for Assigned Names and Numbers
ISP	Internet Service Provider
JCDC	Joint Cyber Defense Collaborative
KYC	Know Your Customer
ML	Machine Learning
NSA	National Security Agency
NSTAC	President's National Security Telecommunications Advisory Committee
ODNI	Office of the Director of National Intelligence

Acronym	Definition
ONCD	Office of the National Cyber Director
R&D	Research and Development
SAR	Suspicious Activity Report
TLD	Top Level Domain
U.S.	United States
U.S.C.	United States Code
USG	United States Government
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Networks

Appendix E. Definitions

Table 6: Definitions

Term	Definition	Source
Business Email Compromise	A type of cybercrime where the criminals send an email message that appears to come from a known source making a legitimate request.	▪ FBI: Business email Compromise
Cloud Computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.	▪ National Institute of Standards and Technology Interagency or Internal Report (NISTIR) 8006 under "cloud computing"
Command and Control	Command and control is defined as a technique used by threat actors to communicate with compromised devices over a network.	▪ Palo Alto Networks
Critical Infrastructure	Sixteen sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.	▪ CISA: Critical Infrastructure Sectors
Customer Proprietary Network Information	The information that telecommunications services acquire about their subscribers. It includes what services they use, as well as the amount and type of usage.	▪ Federal Communications Commission: Privacy/Data Security/Cybersecurity: Customer Proprietary Network Information

Term	Definition	Source
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.	▪ Committee on National Security Systems Instruction (CNSSI) 4009-2015 from National Security Presidential Directive 54 (NSPD-54)/Homeland Security Presidential Directive 23 (HSPD-23) ▪ NIST SP 1800-25B under Cybersecurity from CNSSI 4009-2015 ▪ NSPD-54/HSPD-23 ▪ NIST SP 1800-26B under Cybersecurity from CNSSI 4009-2015 ▪ NSPD-54/HSPD-23 ▪ NIST SP 800-160 Vol. 2 from CNSSI 4009-2015 ▪ NIST SP 800-37 Rev. 2 ▪ NIST SP 800-53 Rev. 5 from OMB Circular A-130 (2016) ▪ NISTIR 7621 Rev. 1 under Cybersecurity from CNSSI 4009-2015

Term	Definition	Source
EO 13984, *Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities*	Directs the Department of Commerce to (i) issue regulations to detect and deter the use of domestic IaaS products in malicious cyber-enabled activities primarily via identity verification requirements and to (ii) coordinate with other US government agencies to impose "special measures" against certain foreign persons and/or foreign jurisdictions.	▪ Federal Register: Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber- Enabled Activities
EO 14028, Improving the Nation's Cybersecurity	Charges multiple agencies, including NIST, with enhancing cybersecurity through a variety of initiatives related to the security and integrity of the software supply chain.	▪ Federal Register: Improving the Nation's Cybersecurity
EO 14086, Enhancing Safeguards for United States Signals Intelligence Activities	Reinforces privacy and civil liberties safeguards for U.S. signals intelligence activities.	▪ Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities | The White House
Hardware	The physical components of an information system.	▪ NIST SP 800-53 Rev. 4 under Hardware CNSSI 4009
Identity and Access Management	(Also known as identity management.) A fundamental cybersecurity concept focused on ensuring "the right people and things have the right access to the right [technology] resources at the right time."	▪ NIST: Identity and Access Management

Term	Definition	Source
Indicators of Compromise	Indicators of Compromise are the digital and informational "clues" that incident responders use to detect, diagnose, halt, and remediate malicious activity in their networks.	▪ CISA: Understanding Indicators of Compromise (IR108)
Industrial Control System (ICS)	General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy)	▪ NIST: Industrial Control System

Term	Definition	Source
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.	▪ Federal Information Processing Standards 200 under Information Technology 40 U.S.C., Sec. 1401
Infrastructure as a Service	Capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components.	▪ NIST: Infrastructure as a Service

Term	Definition	Source
Machine Learning	Machine Learning refers to the field and practice of using algorithms that are able to "learn" by extracting patterns from a large body of data. This contrasts to traditional rule-based algorithms.	▪ General Services Administration: Key AI terminology
Malware	Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.	▪ CNSSI 4009-2015 under malicious logic from Internet Engineering Task Force Request for Comments 4949 V2
Multi-factor Authentication	Multi-factor authentication is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify a user's identity for login.	▪ CISA: Multi-Factor Authentication (MFA)
National Security and Emergency Preparedness	Policies, plans, procedures, and readiness measures that enhance the ability of the U.S. government to mobilize for, respond to, and recover from a national security emergency.	▪ Department of the Interior
Operating System	The software "master control application" that runs the computer. It is the first program loaded when the computer is turned on, and its main component, the kernel, resides in memory at all times. The operating system sets the standards for all application programs (such as the Web server) that run in the computer. The applications communicate with the operating system for most user interface and file management operations.	▪ NIST SP 800-44 Version 2 ▪ NISTIR 7621 Rev. 1 from NIST SP 800-44 Version 2

Term	Definition	Source
Operational Technology	Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.	▪ NIST SP 800-37 Rev. 2
Protocol	A set of rules used by two or more communicating entities that describe the message order and data structures for information exchanged between the entities.	▪ NIST: Protocol
Threat	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or DoS.	▪ NIST SP 800- 53, CNSSI 4009, Adapted
Threat Environment	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.	▪ NIST: Threat

Term	Definition	Source
Verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome).	▪ NIST SP 800-161 under Verification from CNSSI 4009 ▪ ISO 9000 – Adapted ▪ NISTIR 7622 under Verification from CNSSI 4009, ISO 9000 – Adapted
Virtual Private Networks	A virtual network built on top of existing networks that can provide a secure communications mechanism for data and IP information transmitted between networks.	▪ NIST: Virtual Private Network
Zero Trust	A collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.	▪ NIST SP 800-207, https://doi.org/10.6028/NIST.SP.800-207
Zero Trust Architecture	An architecture that treats all users as potential threats and prevents access to data and resources until the users can be properly authenticated and their access authorized.	▪ NIST, https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture

Appendix F. Bibliography

Antonakakis, Manos, Georgia Institute of Technology and Voreas Laboratories. "Lessons Learned from Tracking APTs and Illicit Activities on the Internet." Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, June 6, 2023.

Bagley, Drew, James Perry, and Robert Sheldon, Crowdstrike Holdings. "Infrastructure as a Service Abuse." Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, June 8, 2023.

Bailey, Leonard, Sean Boyle, Katherine Moy, Kimberley Raleigh, and Alison Zitron, Department of Justice. Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, March 30, 2023.

Bank Secrecy Act of 1970. 31 U.S.C. § 5311 *et seq*. (1970). The Bank Secrecy Act | FinCEN.gov

Boscovich, Richard, Chris Compton, David Fosth, Juan Hardoy, and Jason Lyons, Microsoft Corporation. "Microsoft Approach to Countering Fraud and Abuse." Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, June 8, 2023.

Brammer, Zoë, Silas Cutler and Megan Stifel, Institute for Security and Technology. Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, April 6, 2023.

Benda, Paul, and John Carlson, American Bankers Association. "Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors (ADI)." Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, May 2, 2023.

Boyer, Chris, and Brian Rexroad, AT&T. Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, June 6, 2023.

Cloudflare. "What is Credential Stuffing? Credential Stuffing vs. Brute Force Attack," accessed September 11, 2023. https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/

Communications Sector Coordinating Council (CSCC), Cybersecurity and Infrastructure Security Agency (CISA), and Information Technology Sector Coordinating Council (ITSCC). "Working Group One: Extension Period Report, Preliminary Considerations of Paths to Enable Improved Multi-Directional Sharing of Supply Chain Risk Information, September 2021. https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force_multi-directional-sharing-scri_508.pdf

Costello, John, Center for Strategic and International Studies. Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, June 27, 2023.

Creyts, Kyle, Coinbase. Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, April 6, 2023.

Crowdstrike. "Credential Stuffing," March 2022. What is Credential Stuffing? - CrowdStrike

CSCC, CISA, and ITSCC. "Information and Communications Technology Supply Chain Risk Management Task Force Year 2 Report, Status Update on Activities and Objectives of the Task Force," December 2020. https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force_year-two-report_508.pdf

Cybersecurity and Infrastructure Security Agency. "Traffic Light Protocol (TLP) Definitions and Usage." August 22, 2022. https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage

Cybersecurity Information Sharing Act of 2015, 6 U.S.C. §§ 1501–1510 (2015). https://law.justia.com/codes/us/2015/title-6/chapter-6/subchapter-i/

Daniel, Michael, Cyber Threat Alliance. "Malicious Use of U.S. Infrastructure: Perspectives from a Threat Intelligence Sharing Organization." Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, March 21, 2023.

Department of Justice. "Justice Department Announces Court-Authorized Disruption of Snake Malware Network Controlled by Russia's Federal Security Service." May 9, 2023. https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-snake-malware-network-controlled-

Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2523 (1986). Electronic Communications Privacy Act of 1986 (ECPA) | Bureau of Justice Assistance (ojp.gov).

European Data Protection Board. "2022 Coordinated Enforcement Action - Use of cloud-based services by the public sector." January 17, 2023. https://edpb.europa.eu/system/files/2023-01/edpb_20230118_cef_cloud-basedservices_publicsector_en.pdf

Evans, Sean, Department of the Treasury. "The AML Framework in the Prevention, Detection, and Reporting of Illicit Finance." Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, March 21, 2023.

Flynn, Patrick and John Fokker, Trellix. Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, April 20, 2023.

Foreign Intelligence Surveillance Act. 50 U.S.C. §§ 1805, 1842, 1861 (1978). National Security Agency/Central Security Service > Signals Intelligence > FISA (nsa.gov).

Forscey, David, and Michael Garcia, CISA. "Perspectives on Countering Malicious Abuse of Digital Resources." Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, March 14, 2023.

Ginwala, Aadil, Bureau of Industry and Security (BIS), Department of Commerce. "Executive Order 13984 and Infrastructure as a Service Threat." Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, March 7, 2023.

Gucker, David, The Constant Company. Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, May 9, 2023

Hilligoss, Trevor, SpyCloud. Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, April 18, 2023.

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

Kelly, Steve and Elke Sobieraj, National Security Council. Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, February 16, 2023.

Kilmur, Riley, Spur. "Your Infrastructure for Rent." Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, April 20, 2023

Knerr, Casey, MITRE. Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, May 10, 2023.

Koven, Jaqueline Burns and Brian Carter, Chainalysis. "Examining Infrastructure as a Service through Blockchain Analytics." Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, April 13, 2023.

Lazcano, Christina, Aurora Johnson, and David Stern, Joint Cyber Defense Collaborative. "Threat Actor Abuse of U.S.-Based Cloud and Telecommunications Infrastructure." Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, May 4, 2023.

Lefkovitz, Naomi, and Kevin Stine, National Institute of Standards in Technology (NIST). Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, April 11, 2023.

Leong, Jason, and Wolfgang Moser, Federal Bureau of Investigation. "Law Enforcement Perspectives on Nation State Actors and U.S. Infrastructure." Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, March 28, 2023.

Levy, Reg, Tucows. Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, May 30, 2023

McRee, Russ, and Christopher Porter, Google. "Google Threat Intelligence – Abuse of U.S. Infrastructure." Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, June 22, 2023.

Miller-Osborn, Jen, Palo Alto Networks. Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, April 18, 2023.

NSA. "Cybersecurity 2022 Year in Review." December 15, 2022. https://media.defense.gov/2022/Dec/15/2003133594/-1/-1/0/0139_CSD_YIR22_FINAL_LOWSIDE_ACCESSIBLE_FINAL_V2.PDF

NSA. "Cybersecurity Collaboration Center" https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/

Nelson, Steve, Goldman Sachs & Co. "Executive Order 13984—An Origin Story." Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, March 28, 2023.

Oxley, David, Mark Ryland, and Jordana Siegel, Amazon Web Services. Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, June 15, 2023.

Palo Alto Networks. "What is the Principle of Least Privilege?" Accessed September 11, 2023. https://www.paloaltonetworks.com/cyberpedia/what-is-the-principle-of-least-privilege

Privacy Act of 1974, as amended, 5 U.S.C. § 552a (1974). https://www.justice.gov/opcl/privacy-act-1974

Purtill, Mike, Office of the National Cyber Director, and Kristen Lane, Federal Bureau of Investigation. "The Evolving Cyber Threat." Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, March 23, 2023.

Right to Financial Privacy Act, 12 U.S.C. Chapter 35 (1978). https://www.ecfr.gov/current/title-31/subtitle-A/part-14

Ross, Ron, Victoria Pillitteri, Kelley Dempsey, Mark Riddle, and Gary Guissanie, NIST. "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." NIST Special Publication 800-171 Revision 2, February 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

Starzak, Alissa, Cloudflare. Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, June 1, 2023.

Silberstein, Steven, and Bridgette Walsh, Financial Services Information Sharing and Analysis Center. Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, June 13, 2023.

Swire, Peter, Georgia Institute of Technology. Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, April 13, 2023.

Thakur, Vikram, Broadcom. Briefing to the NSTAC Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors Subcommittee, Arlington, VA, April 11, 2023.

The White House. Executive Order 12333, "United States Intelligence Activities." December 4, 1981, National Security Agency/Central Security Service > Signals Intelligence > EO 12333 (nsa.gov).

The White House. Executive Order No. 13984. "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber- Enabled Activities." 86 FR 6837, January 19, 2021.

The White House. Executive Order No. 14028. "Improving the Nation's Cybersecurity." 86 FR 26633, May 12, 2021.

The White House. Executive Order No. 14086. "Enhancing Safeguards for United States Signals Intelligence Activities." 87 FR 62283, October 7, 2022.

The White House. "National Cybersecurity Strategy." March 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

The White House. "National Cybersecurity Strategy Implementation Plan." July 13, 2023. https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf