Risk Factors Comparison 2025-02-13 to 2024-02-15 Form: 10-K

Legend: **New Text** ~~Removed Text~~ Unchanged Text Moved Text Section

Please carefully consider the following discussion of significant factors, events and uncertainties that make an investment in our securities risky. In addition to other information in this Form 10- K, the following risk factors should be carefully considered in evaluating us and our business. When the factors, events and contingencies described below or elsewhere in this Form 10- K materialize, our business, operating results, financial condition, reputation, cash flows or prospects can be materially adversely affected. In such ~~case~~ **cases** , the trading price of our common stock could decline and you could lose part or all of your investment. Additional risks and uncertainties not currently known to us or that we currently deem immaterial may also materially adversely affect our business, operating results, financial condition, reputation, cash flows and prospects. Actual results could differ materially from those projected in the forward- looking statements contained in this Form 10- K as a result of the risk factors discussed below and elsewhere in this Form 10- K and in other filings we make with the SEC. Cybersecurity and Technology Risk Factors Attempted security breaches, including from the exploitation of vulnerabilities, cyber- attacks and Distributed Denial of Service (“ DDoS ”) attacks against our systems and services increase our costs, expose us to potentially material liability, and could materially harm our business and reputation. As an operator of critical internet infrastructure, we experience a high rate of cyber- attacks and attempted security breaches targeting our systems and services, including the most sophisticated forms of attacks, such as advanced persistent threat attacks, exploitation of zero- day vulnerabilities, ransomware attacks, and social engineering attacks. The forms of these attacks are constantly evolving and may involve methods, tools, and strategies that may not have been previously identified and may not have been observed until the moment of launch, or until sometime after, making these attacks virtually impossible to anticipate and difficult to defend against. In addition to external threats, our systems and services are subject to insider threat risks, including physical or electronic break- ins, sabotage, and risks from suppliers, such as consultants and advisors, SaaS providers, hardware, software, and network systems manufacturers, regional internet registries, and other vendors, or from current or former contractors or employees. These threats and any resulting security breaches can arise from intentional or unintentional actions. Our continued exposure to these threats and the potential that they could lead to material liability claims against us requires us to expend significant financial and other resources. We have developed policies, standards, and procedures to identify, protect, detect, respond, and recover from threats posed by cybersecurity risks, and failure to comply with these policies, standards, and procedures by our employees or suppliers could limit our ability to effectively manage threats from these cybersecurity risks. In addition, we must ensure that our employees stay focused on protecting the Company against cybersecurity threats especially in our hybrid work environment, or our ability to effectively manage cybersecurity risks could be impacted. Our failure to effectively manage these security risks, including insider threats, could result in material harm to our business, including loss of or delay in revenues, failure to meet service level agreements, material liability claims, failure to maintain market acceptance, injury to our reputation, and increased costs, and could call into question our ability to preserve the security and stability of the internet. Security vulnerabilities in our systems and our vendors’ systems, including vulnerabilities in third party software and hardware, pose a material risk to our operations. We use externally- developed technology, systems, and services, including both hardware and software, for a variety of purposes, including compute, storage, encryption and authentication, back- office support, and other functions. We have developed policies, standards, and procedures to reduce the impact of security vulnerabilities in system components, as well as at any vendors where our data is stored or processed. However, such measures cannot provide absolute security. ~~While we strive to remediate known vulnerabilities~~ **Vulnerabilities** ~~on a timely basis, such vulnerabilities~~ could be exploited before a vulnerability has been disclosed or before our remediation is effective and if so, could cause systems and service interruptions, data loss and other damages. Our failure to identify, remediate and mitigate security vulnerabilities, including any potential failure to timely replace and upgrade hardware, software, or other technology assets, could result in material harm to our business, including loss of or delay in revenues, failure to meet service level agreements, material liability claims, failure to maintain market acceptance, injury to our reputation, increased costs, and call into question our ability to preserve the security and stability of the internet. In addition, our networks have been, and likely will continue to be, subject to DDoS attacks. Recent industry experience has demonstrated that DDoS attacks continue to grow in size and sophistication and have the ability to widely disrupt internet services. **We** ~~While we have adopted mitigation techniques, procedures, and strategies to defend against DDoS attacks, and~~ have successfully mitigated DDoS attacks to date **; however** , there can be no assurance that we will be able to defend against every attack, especially as the attacks increase in size and sophistication. Any attack, even if only partially successful, could disrupt our networks, increase response time, negatively impact our ability to meet our service level agreements, and generally impede our ability to provide reliable service to our customers and the broader internet community. We have historically incurred, and will continue to incur, significant costs to enable our infrastructure to process levels of attack traffic that can be substantially larger than our normal transaction volume. We are employing new technologies and new and different services and capabilities to help mitigate DDoS attacks. If these new technologies, services and capabilities are not effective, our infrastructure could **be** ~~bedisrupted~~ -- **disrupted** , our response times could increase, our ability to meet our service ~~level agreements~~ **levelagreements** could be negatively impacted, and our ability to provide reliable service to our customers and the broader internet community could be impeded. In addition, we are subject to social engineering attacks including phishing, spear phishing, whaling, vishing, smishing, and domain spoofing, which are designed to entice people to divulge sensitive information or take actions that, if successful, could pose a material risk to our operations. The number of such attacks is increasing. Recent advances in artificial intelligence have increased the sophistication of these types of attacks as

attackers are able to create more personalized and targeted communications using information derived from people' s relationships, online behavior and preferences. Social engineering attacks have occurred in concert with ransomware attacks. ~~While~~ **The various measures** we **take to mitigate cyber- attacks, including our** ~~deploy~~ **deployment of** advanced tools and **implementation of redundant architecture and multiple recovery solutions, as well as** ~~conduct~~ **conducting** continuous security awareness training to address social engineering attacks ~~, such measures~~ **and periodic exercises to mitigate the threat of ransomware** cannot provide absolute security. **We** ~~Similarly, although we implement redundant architecture and multiple recovery solutions, and conduct periodic exercises to mitigate the threat of ransomware, we~~ still may be subject to successful ~~ransomware~~ **cyber** attacks. Our failure to prevent such attacks, including any successful social engineering attack, could result in our inability to meet our service ~~legal~~ **level** agreements and could otherwise materially harm our business, including from legal claims, governmental investigations and scrutiny, injury to our reputation, and increased costs. We do not maintain specific reserves for security breaches, cyber- attacks and DDoS attacks against our systems and the amount of insurance coverage we maintain may be inadequate to cover claims or liabilities relating to such attacks. We may introduce undetected or unknown defects into our systems or services, which could materially harm our business and harm our vendors or our customers. Despite testing, services as complex as those we offer or develop could contain undetected defects or errors, which could result in service outages or disruptions, compromised customer data, including DNS data, diversion of development resources, injury to our reputation, legal claims, increased insurance costs or increased service costs. Performance of our services, whether or not defective, could have unforeseen or unknown adverse effects on the networks over which they are delivered, on internet users and consumers, and on third- party applications and services that use our services, any of which could result in legal claims against us. While we strive to prevent, detect and remediate defects or errors, they can and do occur and they could result in our inability to meet customer expectations in a timely manner, failure to meet our service level agreements, injury to our reputation, and increased costs. Our infrastructure and services are subject to vulnerabilities in the global routing system for the internet, as well as risks arising from internet services providers' increasing adoption of the Resource Public Key Infrastructure system. Routing on the internet depends on the Border Gateway Protocol (" BGP "), which is a protocol that relies on networks within the internet infrastructure acting in a trustworthy manner when sharing information about destinations for connectivity and the routing of internet traffic. As a trust- based protocol, BGP has a number of vulnerabilities that may lead to outages or disrupt our services, including as a result of " route hijacks " that involve accidental or malicious rerouting of internet traffic, or " route leaks " that involve the malicious or unintentional propagation of routing information beyond the intended scope of the originator, receiver, and / or one of the networks along the route' s path. Both route hijacks and route leaks can result in partial or full rerouting of internet traffic for the impacted destinations. These types of events, which are generally beyond our control, could enable an array of attack conditions or service disruptions, and could result in adverse publicity and adversely affect the public' s perception of the security of e- commerce and communications over the internet, as well as of the security or reliability of our services. To address internet routing system vulnerabilities, many internet service providers have adopted and apply internet reachability policies based on a system known as the Resource Public Key Infrastructure (" RPKI ") operated by the regional internet registries (" RIRs "). The RIRs allocate internet number resources, such as internet protocol addresses, to enterprises and network operators. We have limited visibility into the maturity of and investment in the RIRs' operational and security controls, which are outside of our control. When the availability, integrity, or confidentiality of any of the information in the RPKI system, or systems used to maintain and administer RPKI data and systems, are impacted or otherwise compromised in any of the RIRs, or any network operator that is a relying party of the RPKI system, or the operations or ingestion of data from the RPKI system are otherwise impacted by a known or unknown vulnerability, our services may be negatively impacted. Such impacts may include degraded or full loss of reachability of service addresses in the global internet routing system, resulting in degradation or complete loss of availability of our registration and resolution services. A compromise of the RPKI system and related services, or unintentional or unauthorized manipulation of data therein, may also result in other denial of service attack conditions for our infrastructure and services. The systemic dependencies introduced by the RPKI system and by the relying parties of the RPKI system, including internet service providers, are outside of our control, and systems that depend upon the RPKI may be only as secure as the weakest elements of the RPKI system. Contracting with RIRs for the provision of and access to RPKI services carries material operational risks, as described above, as well as material contractual risks, which may expose us to service disruptions and material liability. We could encounter system interruptions or ~~systems~~ **system** failures resulting from activities beyond our direct control that could materially harm our business. We depend on the uninterrupted operation of our various systems, secure data centers, points of presence around the world and other computer and communication networks. Our systems and operations are vulnerable to damage or interruption from power loss, transmission cable cuts and other telecommunications failures, damage or interruption caused by fire, earthquake, and other natural disasters, intentional acts of vandalism, terrorist attacks, unintentional mistakes, or errors. Our systems and operations also face risks inherent in, or arising from, the terms and conditions of our agreements with service providers to operate our networks and data centers. We are also subject to the risk of state suppression of internet operations. Any of these scenarios could create potential liability and exposure, including from a failure to meet our service level agreements, and could decrease customer satisfaction, harming our business, or resulting in adverse publicity and damage to our reputation or call into question our ability to preserve the security and stability of the internet. Our data centers, our data center systems, including the Shared Registration Systems located at our data centers, and our resolution systems are vulnerable to damage or interruption, which could impede our ability to provide our services, expose us to material liability, and materially harm our reputation. Most of the computing infrastructure for our Shared Registration System is located at, and most of our customer information is stored in, data centers we own or lease ~~and operate. In 2019, we expanded some of our data center services to a leased data center facility~~. These data centers **, which are concentrated in the same geographic region,** are vulnerable to damage or interruption, including from natural disasters, such as fires, earthquakes, hurricanes, and floods, power loss, hardware or system failures,

physical or electronic break- ins, human error or interference. We are also regularly updating and enhancing our network architecture in ~~several of~~ our ~~new and existing~~ data centers and globally distributed resolution systems. If our data center facilities or the updated network architectures, hardware or software upgrades, or security controls do not operate as expected, including the ability to quickly switch over between sites, we could experience service interruptions or outages. A failure in the operation of our Shared Registration System could result in the inability of one or more registrars to register or manage domain names for a period of time. If such a registrar has not implemented robust services in a manner that preserves transactions until processed by the registry, then the failure in the operation of our Shared Registration System could result in permanent loss of transactions at the registrar during that period. A failure in the operation of our Shared Registration System could also impact our ability to provide up- to- date information in our globally distributed resolution systems, which could result in breaches of our service level agreements pertaining to our resolution services and impact the resolution of domain names on the internet. We do not carry insurance or designated financial reserves for such interruptions. In addition, our services depend on the secure and efficient operation of the internet connections to and from customers to our Shared Registration System residing in our secure data centers as well as our globally distributed resolution systems. These connections depend upon the secure and efficient operation of internet service providers, internet exchange point operators, and internet backbone service providers. Such providers have encountered periodic operational problems or experienced outages in the past beyond our scope of control and may continue to encounter problems and outages or may choose to discontinue their service. If the providers that our connections depend upon do not protect, maintain, improve, and reinvest in their networks or present inconsistent, incorrect, or invalid data regarding routing information or DNS responses through their networks, our business could be harmed. A failure in the operation or update of the root zone servers **that we operate** , the root zone file, the Root Zone Management System, the TLD name servers, the TLD zone files that we operate, or other network functions, could result in, among other problems, (1) a DNS resolution or other service outage or degradation, (2) the deletion of one or more gTLDs or ccTLDs from the internet, (3) the deletion of one or more second- level domain names from the internet, or (4) a misdirection of one or more domain names to different servers. A failure in the operation or update of the supporting cryptographic and other operational infrastructure that we maintain could result in similar consequences. Any of these problems or outages could create potential material liability and exposure from litigation and investigations, could result in a failure to meet our service level agreements, and could decrease customer satisfaction, harming our business. These problems could also result in adverse publicity, decrease the public' s trust in the security of e- commerce and other forms of online presence, or call into question our ability to preserve the security and stability of the internet. We retain certain customer and employee information in our data centers and various domain name registration systems. Any physical or electronic break- in or other security breach or compromise of the information stored at our data centers or domain name registration systems may jeopardize the security of information we retain or that is retained in the computer systems and networks of our customers. In such an event, we could face material liability and exposure from litigation and investigations, fail to meet service level agreements, or be at risk of losing various security and standards- based compliance certifications needed for operation of our businesses, and customers could be reluctant to use our services. Any such outcomes could also adversely affect our reputation and harm our business or cause financial losses that are either not insured against or not fully covered through any insurance. We face risks from the operation of the root server system and our performance of the Root Zone Maintainer functions under the RZMA. Although the overall root server system is redundant and dispersed, ~~a~~ **an infrastructure or services** failure or ~~interruption~~ **other disruption of one or more organizations involved** in the operation of the root server system could impact the effectiveness of our. com and. net authoritative servers and therefore negatively impact directory services necessary for the operation of the internet. We also have an important operational role in support of a key Internet Assigned Numbers Authority (" IANA ") function as the Root Zone Maintainer. In this role, we provision and publish the authoritative root zone data and make it available to all root server operators under the RZMA with ICANN. If we make errors in the publication of the root zone or experience operational issues that impact the timeliness of updates to the root zone data, we may be subject to material claims challenging the RZMA or our performance under it, including tort claims, and we may not have immunity from, or sufficient indemnification or insurance for, such claims. Economic and Competition Risk Factors Deterioration of..... 10- K for further information. Contractual, Regulatory, Legal and Compliance Risk Factors Any loss or modification of our right to operate the. com and. net gTLDs could have a material adverse impact on our business and result in loss of revenues. Substantially all of our revenues are derived from our operation of the. com gTLD under our Cooperative Agreement with the DOC and our. com Registry Agreement as well as our operation of the. net gTLD under our. net Registry Agreement. Any loss or modification of our right to operate the. com and. net gTLDs could materially and adversely impact our ability to conduct our business and result in loss of revenues. Our. com and. net Registry Agreements contain " presumptive " rights of renewal upon the expiration of their current terms on November 30, ~~2024~~ **2030** and June 30, 2029, respectively. ICANN could refuse to renew upon expiration or terminate our. com Registry Agreement or our. net Registry Agreement if, upon proper notice, (1) we fail to cure a fundamental and material breach of certain specified obligations, and (2) we fail to timely comply with a final decision of an arbitrator or court. Additionally, each of the. com and. net Registry Agreements provide that if certain terms of these agreements are not similar to such terms generally in effect in the registry agreements of the five largest gTLDs, then a renewal of these agreements would be upon terms reasonably necessary to render such terms to be similar to the registry agreements for those other gTLDs. Any such terms, if they apply, could be unfavorable to us and have a material adverse impact on our business. Standard renewals of the. com Registry Agreement do not require further DOC approval, although the prior written approval of the DOC is required for the removal of, or any changes to the pricing section (other than as approved in Amendment 35 to the Cooperative Agreement), and for changes to certain other specified terms whether such removal or changes are made at a renewal or otherwise. We can provide no assurances that DOC approval would be provided upon our request for any of these changes. In addition, under Amendment 35 to the Cooperative Agreement, we have agreed to continue to operate the. com gTLD in a content- neutral manner and to work within ICANN

processes to promote the development of content- neutral policies for the operation of the DNS, and under our binding letter of intent with ICANN, we have agreed to work with the ICANN community to develop certain best practices and other commitments for the security, stability and resiliency of the DNS and the internet. Such policies and processes could expose us to compliance costs and substantial liability and result in costly and time- consuming investigations or litigation. Changes or challenges to the pricing provisions in the. com Registry Agreement could have a material adverse impact on our business. Under the terms of the. com Registry Agreement, we may increase the annual fee of each. com domain name registration or renewal by up to 7 % over the previous year in each of the final four years of each six- year period. We can provide no assurances that we will exercise such right to increase the annual fee. In addition to this contractual right, we are entitled to increase the annual fee of each. com domain name registration or renewal by up to 7 % due to the imposition of any new specifications or policies adopted by ICANN pursuant to the procedures set forth in its bylaws and due process (" Consensus Policies ") or to a documented extraordinary expense resulting from an attack or threat of attack on the security and stability of the DNS (an " Extraordinary Expense "). In addition, our ability to increase the price for. com domain name registrations and renewals due to a Consensus Policy or Extraordinary Expense may occur only in years in which we do not increase the price for. com domain name registrations and renewals as described above. It is uncertain whether circumstances would arise that would permit us to take a price increase due to a Consensus Policy or Extraordinary Expense, or if they do, whether we would seek to increase the price for. com domain name registrations for this reason. A failure to seek and obtain a price increase due to a Consensus Policy or Extraordinary Expense, when applicable, could negatively affect our operating results. We also have the right under the Cooperative Agreement to seek the removal of these pricing restrictions on the. com gTLD if we demonstrate to the DOC that market conditions no longer warrant these restrictions. However, we can provide no assurances whether we will seek the removal of these restrictions, or whether the DOC would approve the removal of these restrictions. Our. com Registry Agreement, **and the Cooperative Agreement,** including ~~its~~ **their** pricing provisions, ~~has faced~~ **have been challenged** , and could face **challenges** in the future, ~~challenges~~ **through publicity campaigns** , ~~including possible~~ **governmental scrutiny, media interest,** legal challenges, or challenges under ICANN' s accountability mechanisms **. Such challenges have arisen** , **and could in the future, arise** from ~~ICANN~~ **trade organizations, the media** , registrars, registrants, and others, **particularly when** ~~and any adverse outcome from~~ these **agreements are being renewed. These** challenges **, if successful, and even when unmeritorious and / or unsuccessful,** could have a material adverse effect on our business. Government regulation and the application of new and existing laws in the U. S. and internationally may slow business growth, increase our costs of doing business, create potential material liability and could have a material adverse effect on our business. Application of new and existing laws and regulations in the U. S. or internationally to the internet or the domain name industry have imposed and may in the future impose new costs and new restrictions on our business. **. In the U. S., new or modified Executive Orders or legislation involving the internet, cybersecurity, or in other areas could result in new obligations that could negatively impact our business. In addition,** ~~Laws~~ **laws** and regulations, including those designed to restrict who can register and who can distribute domain names or to require registrants to provide additional documentation to register domain names, have, and may in the future, impose significant additional costs on our business and subject us to additional liabilities or could prevent us from operating in certain jurisdictions. For example, the government of China has indicated that it will issue, and has issued, new regulations, and it has begun to enforce existing regulations differently, including by directing certain implementation models for registry services, that impose additional costs on, and risks to, our provision of registry services in China. These regulations are impacting the demand for domain name registrations in China. These regulations require registries, including us, and China- based registrars, to obtain a government- issued license for each gTLD or ccTLD operating in China. Any failure to obtain or renew the required licenses, or to comply with any license requirements or any updates thereto, or any failure to comply with these regulations or directives, by us or our China- based registrars, could result in significant harm to our business in China including the suspension of some or all of our registry services in China. We are also subject to changing laws and regulations that impact whether, how, and under what circumstances we may transfer, process and / or receive certain data that is critical to our operations, including data shared between countries or regions in which we operate and data shared among our products and services. For example, ~~following~~ the ~~invalidation of the U. S.- EU Safe Harbor by the European Court of Justice (" EUCJ ") in 2015, the European Union and United States agreed to an alternative framework for data transferred from the European Union to the United States, called Privacy Shield. In 2018, Privacy Shield was also invalidated by the EUCJ. In 2022, the United States and European Union announced a new, but undefined~~ data transfer ~~framework~~ **frameworks , which once finalized, also could be between the U. S. and E. U. have been** subject to ~~further~~ legal challenges **, which has created uncertain legal obligations** . New laws, regulations, directives or ICANN ~~polices~~ **policies** that require us to obtain and maintain personal information of registrants of domain names in the. com and. net gTLDs could impose material compliance costs and could create new, material legal and ~~others~~ **other** risks to our business. If we are required to, or choose to, obtain and maintain personal information of registrants of domain names in the. com and. net gTLDs we could be required to incur significant compliance and legal costs as a result of GDPR and other similar regulations. For example, ~~we could incur material costs~~ **in 2023, the European Union adopted the Network and Information Security Directive (" NIS 2 ") that addresses registrant data. Our current obligations do not require us** to ~~protect such~~ **obtain and maintain personal** information ~~from unauthorized disclosure and~~ **of registrants of domain names. Specific E. U. member state implementations of NIS 2 could create uncertainty about** , ~~under GDPR~~ **or change** , **these obligations** ~~to ensure authorized disclosures are permitted~~ . Failure to properly protect such information, **if obtained,** or failure to comply with GDPR **or NIS 2** , could expose the Company to material costs and penalties. In addition, new obligations to obtain and maintain personal information of registrants in the. com and. net gTLDs could conflict with certain laws and regulations that may require such personal information be maintained solely within the jurisdiction of the data subject. In addition, any such new obligations could increase the cost and risks associated with complying with regulations that require verification of registrant personal information, including for purposes of complying with

the economic and trade sanctions programs administered by the Office of Foreign Assets Control (“ OFAC ”). Such laws, regulations, directives or ICANN policies, could give rise to significant claims, inquiries, investigations or other actions against us, which could result in significant costs, damages, fines or penalties and could delay the development of new products, change our current business practices, result in negative publicity, require significant management time and attention, all or any of which could materially harm our business. Our international operations expose us and our business to additional economic, legal, regulatory and political risks that could have a material adverse impact on our revenues and business. A significant portion of our revenues is derived from customers outside the U. S. Our business operations in international locations have required, and will continue to require, significant management attention and resources. We may also need to tailor some of our services for a particular location and to enter into international distribution and operating relationships. We may fail to maintain our ability to conduct business, including potentially material business operations in some international locations, or we may not succeed in expanding our services into new international locations or expand our presence in existing locations. Failure to do so could materially harm our business. Moreover, local laws and customs in many countries differ significantly from those in the U. S. In many foreign countries, particularly in those with developing economies, it is common for others to engage in business practices that are prohibited by our internal policies and procedures or U. S. law or regulations applicable to us. There can be no assurance that our employees, contractors and agents will not take actions in violation of such policies, procedures, laws and / or regulations. Violations of laws, regulations or internal policies and procedures by our employees, contractors or agents could result in financial reporting problems, investigations, fines, penalties, or prohibition on the importation or exportation of our products and services and could have a material adverse effect on our business. In addition, we face risks inherent in doing business internationally, including: • competition with companies in international locations or other domestic companies entering international locations in which we operate, as well as local governments actively promoting ccTLDs that we do not operate; • political and economic tensions between governments and changes in international trade policies and / or the economic and trade sanctions programs administered by OFAC of the U. S. Department of the Treasury; • tariffs and other trade barriers and restrictions; • difficulties in staffing and managing international operations; • potential problems associated with adapting our services to technical conditions existing in different countries; • additional vulnerability from terrorist groups targeting U. S. interests abroad; • potentially conflicting or adverse tax consequences; • reliance on third parties in international locations in which we only recently started doing business; and • potential concerns of international governments or customers and prospects regarding doing business with U. S. technology companies due to alleged U. S. government data collection policies. Political tensions between the United States and China **, including tensions resulting from tariffs or proposed tariffs,** in particular may pose additional risks to our business in China. The U. S. government has imposed restrictions on certain Chinese companies and on trading in certain technologies. The Chinese government has announced actions that, if implemented, could impose additional restrictions on the operations of non- Chinese companies in China. These and **possible** future government actions could impact our ability to operate in China and may cause our management’ s attention to be diverted, our reputation to be damaged, or our business in China to be adversely affected. Changes in, or interpretations of, tax rules and regulations or our tax positions may materially and adversely affect our income taxes. We are subject to income taxes in both the U. S. and numerous international jurisdictions. Significant judgment is required in determining our worldwide provision for income taxes. In the ordinary course of our business, there are many transactions and calculations where the ultimate tax determination is uncertain. Our effective tax rates may fluctuate significantly on a quarterly basis because of a variety of factors, including changes in the mix of earnings and losses in countries with differing statutory tax rates, changes in our business or structure, changes in tax laws that could adversely impact our income or non- income taxes or the expiration of or disputes about certain tax agreements in a particular country. We are subject to audit by various tax authorities. In accordance with U. S. GAAP, we recognize income tax benefits, net of required valuation allowances and accrual for uncertain tax positions. Although we believe our tax estimates are reasonable, the final determination of tax audits and any related litigation could be materially different than that which is reflected in historical income tax provisions and accruals. Should additional taxes be assessed as a result of an audit or litigation, an adverse effect on our results of operations, financial condition and cash flows in the period or periods for which that determination is made could result. The Organization for Economic Cooperation and Development (“ OECD ”) continues to issue guidance that will provide a long- term, multilateral proposal on the taxation of the digital economy. Certain countries **, including our major international tax jurisdictions,** have enacted ~~and other countries may enact~~ legislation based on the OECD’ s guidance ~~that could~~ **. To date the legislation has had a limited** impact **on us, but** the ~~taxation~~ **impact** of ~~the digital economy~~ **future legislation is uncertain** . Similarly, some international tax jurisdictions, independent of the OECD, have enacted or may enact new tax regimes aimed at income resulting from digital services. Although we cannot predict the nature or outcome of such changes or the likelihood of such legislative proposals being adopted in the U. S. or throughout the world, any or all of these changes in tax laws **, including but not limited to changes in scope of OECD’ s Pillar One, as well as new guidance issued and enacted pertaining to OECD’ s Pillar Two,** could increase our taxes and adversely impact our financial condition and cash flow. Our business faces risks arising from ICANN’ s consensus and temporary policies, technical standards and other processes. Our Registry Agreements with ICANN require us to implement Consensus Policies and changes mandated by ICANN through temporary specifications or policies (“ Temporary Policies ”). ICANN could adopt Consensus Policies or Temporary Policies that (1) are unfavorable to us as the registry operator of. com,. net and other gTLDs we operate, (2) are inconsistent with our current or future plans, (3) impose substantial costs on our business, (4) subject the Company to additional legal risks, or (5) affect our competitive position. These Consensus Policies or Temporary Policies could have a material adverse effect on our business. Our Registry Agreements with ICANN require us to implement and comply with various technical standards and specifications published by the Internet Engineering Task Force (“ IETF ”). ICANN could impose requirements on us through changes to these IETF standards, or new standards, that are inconsistent with our current or future plans, that impose substantial costs on our business, that subject the Company to

additional legal risks, or that affect our competitive position. Any such changes to the IETF standards, or new standards, could have a material adverse effect on our business. Weakening of, or changes to, the multi- stakeholder form of internet governance could materially and adversely impact our business. The internet is governed under a multi- stakeholder model comprising civil society, the private sector, including for- profit and not- for- profit organizations such as ICANN, governments, including the U. S. government, academia, non- governmental organizations and international organizations. If ICANN fails to uphold, or if the multi- stakeholder model is significantly redefined, it could harm our business. For example, certain governments, governmental organizations, and private actors continue to express dissatisfaction with the multi- stakeholder form of internet governance and have proposed alternatives including oversight by the United Nations or by international treaties. Furthermore, national legislation has been proposed on topics such as information security and access to personal information that effectively supplants the multi- stakeholder process for policy development in the DNS. Substantially weakening or replacing the multi- stakeholder form of internet governance could materially harm our business. In addition, in 2016 the U. S. government transferred key internet functions to ICANN, who adopted new and enhanced accountability mechanisms in its bylaws such as the creation of the Empowered Community. There can be no assurance that the removal of the U. S. government oversight of these key functions, or the changes to ICANN' s bylaws, will not negatively impact our business. Claims, lawsuits, audits or investigations in which we are or could become involved may result in material adverse outcomes to our business. We are, and may in the future become, involved in claims, lawsuits, audits, and investigations, including intellectual property litigation and infringement claims. Litigation is inherently unpredictable, and unexpected judgments or excessive verdicts do occur. In addition, proceedings that we initially view as immaterial could prove to be material. Adverse outcomes in lawsuits, audits and investigations, could result in significant monetary damages, including indemnification payments, or injunctive relief that could adversely affect our ability to conduct our business, and may have a material adverse effect on our financial condition, results of operations and cash flows. For example, we are engaged in activities to help mitigate security threats and other forms of DNS abuse in the gTLDs and ~~ccTLDs~~ **ccTLD** we operate and we are involved in community efforts that ~~could~~ **have** ~~increase~~ **increased** and ~~expand~~ **expanded** such activities **to** ~~including~~ **include** ~~potential new~~ contractual obligations. **For** ~~Such activities include, for~~ example, **we** ~~receiving~~ **receive** reports of suspected threats and abuse ~~from appropriate " trusted notifiers " (typically involving national~~ and **we** ~~international law enforcement) and notifying~~ --- **notify** registrars or others of domain names associated with suspected malicious or illegal activity. **We** ~~Our activities~~ may also ~~include disabling~~ **disable** one or more domain names in the gTLDs or ~~ccTLDs~~ **ccTLD** we operate including in response to **reports of suspected threats and abuse,** governmental directives and **court** orders in those jurisdictions in which we operate. Activities such as these have resulted in, and could in the future result in, significant litigation and could harm our reputation. Given the inherent uncertainties in litigation, even when we are able to reasonably estimate the amount of possible loss or range of loss and therefore record an aggregate litigation accrual for probable and reasonably estimable loss contingencies, the accrual may change in the future due to new developments or changes in approach. In addition, such claims, lawsuits, audits and investigations could involve significant expense and diversion of management' s attention and resources from other matters **Economic and Competition Risk** Factors ~~Challenging~~ **Deterioration of economic conditions,particularly in China,continues to negatively impact our business.Our business is,and will likely continue to be,adversely affected by the deterioration in** global economic conditions **,including high** ~~have in the past and may in the future negatively impact our business.Factors such as~~ inflation,interest rates, **and** currency fluctuations, ~~trade barriers,tariffs,~~ **as well as impacts from** war,civil unrest,and other political and economic developments ~~and their impact on global economic conditions have in the past and may in the future negatively impact our business~~ .In particular, **these conditions are negatively impacting our business in China,where** demand for our services has substantially declined ~~in~~ **due to worsening economic conditions within** China and **from** ~~may continue to decline further due to lower economic growth and as a result of~~ Chinese regulatory mandates that make it more difficult to register a domain name or establish an online presence using a domain name.The overall economic impact,severity and duration of these conditions,as well as the timing,strength,and sustainability of any ~~future economic growth or~~ recovery,are not known at this time,and are not within the Company' s control.The business environment is highly competitive and,if we do not compete effectively,we may suffer material adverse impact to our business,including lower demand for our products,reduced gross margins,and loss of market share.We face competition from services that provide an online identity or presence,including other gTLDs and ccTLDs.In order to remain competitive,we must continually demonstrate the security,stability,and resiliency of our services and must adopt and support new technologies to adapt our services to changing **technologies** ~~cybersecurity threats,regulations,application environments~~ ,market conditions,and our customers' and internet users' preferences and practices.Also to remain competitive,we have undertaken important initiatives such as our efforts to acquire the.web gTLD,and we may in the future undertake other important initiatives.Any of these initiatives require significant resources,can subject us to regulatory scrutiny and / or negative publicity,and divert management attention from our existing business.Such undertakings,including our efforts to acquire the.web gTLD,may be unsuccessful and costly.In addition,competing technologies developed by others or the emergence of new industry standards may adversely affect our competitive position or render our services or technologies noncompetitive or obsolete.Finally,consolidation within our industry has occurred and is likely to continue to occur.Our ability to participate and benefit from such consolidations may be limited and consolidation within our industry among our competitors could harm our competitive position and adversely impact our business.We have been designated as the registry operator for certain new gTLDs,including certain IDN gTLDs.Our new gTLDs may not be as or more successful than the new gTLDs obtained by our competitors.In addition,our new gTLDs may face additional universal acceptance and usability challenges and it is possible that resolution of domain names within some of these new gTLDs may be blocked within certain state or organizational environments,challenging universal resolvability of these domain names and their general acceptance and usability.See the " Competition " section in Part I,Item 1 of this Form 10- **K for further information.** . Strategic, Business and Operating Risk Factors The evolution of technologies or internet practices and behaviors, the adoption

of substitute technologies, or wholesale price increases of domain names in the gTLDs we operate may materially and negatively impact the demand for the domain names for which we are the registry operator. Technologies relating to online presence, including social media, mobile devices, apps, and search engines, have evolved and continue to evolve, changing the internet practices and behaviors of consumers and businesses. These ongoing changes can negatively impact the demand for our domain names. In addition, registrants purchase domain names for a variety of reasons, including personal, commercial, and investment reasons. Changes in the motivation of domain name registrants can negatively impact our business. Technology changes to web browser or internet search technologies could reduce demand for domain names. Similarly, if internet users' preferences or practices shift away from recognizing and relying on web addresses or if internet users were to significantly decrease the use of web browsers in favor of applications to locate and access content, demand for domain names in the gTLDs we operate could be negatively impacted. Demand for domain names in the gTLDs we operate could be negatively impacted by new technologies that significantly decrease the use of traditional domain names to present and protect an online identity. New technologies that encourage internet users to expand the use of third- level domains or alternative identifiers, such as identifiers from social networking, e- commerce platforms and microblogging sites, could also negatively impact the demand for domain names in the gTLDs we operate. In addition, the demand for domain names in the gTLDs we operate could be impacted by alternative namespaces with domain- name- like identifiers that are operated outside the single authoritative DNS root zone, including blockchain namespaces. To the extent that web browsers, applications, DNS registrars and DNS resolvers recognize and support such namespaces, and that internet users are able to perform online operations with identifiers from such namespaces, demand for domain names in gTLDs and ccTLDs in the single authoritative DNS root zone, including the gTLDs we operate, could be negatively impacted. To the extent that alternative namespaces introduce user confusion about the relationship between identical or similar- looking identifiers in these namespaces and domain names in the DNS, demand for domain names and user confidence in the value of domain names as unique identifiers could also be negatively impacted. **In addition, applications using artificial intelligence could be transformational in ways that cannot be predicted at this time. To the extent such applications impact the demand for domain names, it could have a material impact on our business.** Some registrars and registrants purchase and resell domain names at an increased price in a secondary market. Adverse changes in the resale value of domain names, changes in the business models for such domain name registrars and registrants, or other factors, including regulations limiting the resale of domain names, could result in a decrease in the demand and / or renewal rates for domain names in the gTLDs we operate. Some registrars and registrants seek to generate revenues by registering domain names specifically for website advertising. Changes in the way these registrars and registrants are compensated (including changes in methodologies and metrics) by advertisers and advertisement placement networks, such as Google, Baidu and Bing, have adversely affected, and may continue to adversely affect the market for domain names used for this purpose, which has resulted in, and may continue to result in, a decrease in demand and / or the renewal rate for such domain names. In addition, if spending on online advertising and marketing is reduced, this may result in a further decline in the demand for domain names used for this purpose. Under the terms of the. com and. net Registry Agreements, as amended, we are permitted to increase the annual fee of each. com and. net domain name registration or renewal according to the provisions in these agreements. To the extent we increase our prices, there could be a decrease in the demand and / or renewal rates for. com or. net domain names. If we fail to expand our services into developing and emerging economies in international locations, our business may not grow. We seek to serve new, developing, and emerging economies in international locations to grow our business. These economies are rapidly evolving and may not grow or even if they do grow, our services may not be widely used or accepted there. Accordingly, the demand for our services in these locations is uncertain. Factors that may affect acceptance or adoption of our services in these locations include: • regional internet infrastructure development, expansion, penetration and adoption, and the development, maturity and depth of our sales channels; • acceptance and adoption of substitute products and services that enable online presence without a domain name, including social media, e- commerce platforms, website builders and mobile applications; • increased acceptance and adoption of other substitute products and services, including ccTLDs or other gTLDs; • public perception of the security of our products and services; • the use of mobile applications as the primary engagement mechanism for navigating the internet; and • government regulations affecting the internet, internet access and availability, domain name registrations or the provision of registry services, data security, privacy, or data localization, e- commerce or telecommunications. If our services are not widely accepted or adopted in these locations, our business may not grow. Our business depends on registrars and their resellers maintaining their focus on marketing our products and services. All of the domain name registrations and renewals for the registries we operate occur through registrars. Registrars and their resellers engage in substantial marketing efforts to increase the demand and / or renewal rates for domain names as well as their own associated offerings. Consolidation in the registrar or reseller industry or changes in ownership, management, or strategy among individual registrars or resellers, including vertical integration by registrar or reseller industry participants, could result in significant changes to their businesses, operating models, and cost structures. These changes could include reduced marketing efforts for the gTLDs we operate or other operational changes that could adversely impact the demand and / or the renewal rates for the domain names for which we are the registry operator. With the introduction of new gTLDs, many of our registrars and resellers have chosen to, and may continue to choose to, focus their short- or long- term marketing efforts on these new offerings and / or reduce the prominence or visibility of our products and services on their e- commerce platforms. Our registrars and resellers sell domain name registrations of other competing registries, including new gTLDs, and some also sell and support their own services for websites such as email, website hosting, and other services. Our registrars and resellers may be more motivated to sell to registrants to whom they can also market their own services. To the extent that registrars and resellers focus more on selling and supporting their services and less on the registration and renewal of domain names in the gTLDs we operate, our revenues could be adversely impacted. Our ability to successfully market our services to, and build and maintain strong relationships with, new and existing registrars or resellers is a factor upon which successful operation of our business is

dependent. If we are unable to keep a significant portion of their marketing efforts focused on selling registrations of domain names in the gTLDs we operate, as opposed to other competing gTLDs, including the new gTLDs, or their own services, our business could be harmed. We depend on highly skilled employees to maintain and provide innovative solutions for our business, and our business could be materially harmed if we are not able to attract and retain such qualified talent. Our business is highly technical and requires individuals skilled and knowledgeable in unique technologies, configurations, operating systems, and software development tools. We depend on the knowledge, experience, and performance of these employees and leaders to effectively manage and provide innovative solutions for our business. For example, we require employees with expertise in DNS operations and with certain cybersecurity specialties. Because such employees are in high demand by our competitors and other companies, we must be able to attract, integrate, retain and motivate such highly skilled employees and leaders. Failure to attract and retain such employees and to effectively implement succession plans for these employees could harm our business. Intellectual Property Risk Factors We rely on our intellectual property rights to protect our proprietary assets, and any failure by us to protect or enforce, or any misappropriation of, our intellectual property could materially harm our business. Our success depends in part on our internally developed technologies and related intellectual property. Despite our precautions, it may be possible for an external party to copy or otherwise obtain and use our intellectual property without authorization. Furthermore, the laws of other countries may not protect our proprietary rights in those countries to the same extent U. S. law protects these rights in the U. S. In addition, it is possible that others may independently develop substantially equivalent intellectual property. If we do not effectively protect our intellectual property, our business could suffer. Additionally, we have filed patent applications with respect to some of our technology in the U. S. Patent and Trademark Office and patent offices outside the U. S. Patents may not be awarded with respect to these applications and even if such patents are awarded, third parties may seek to oppose or otherwise challenge our patents, and such patents' scope may differ significantly from what was requested in the patent applications and may not provide us with sufficient protection of our intellectual property. In the future, we may have to resort to litigation to enforce and protect our intellectual property rights, to protect our trade secrets or to determine the validity and scope of the proprietary rights of others. This type of litigation is inherently unpredictable and, regardless of its outcome, could result in substantial costs and diversion of management attention and technical resources. Some of the software and protocols used in our business are based on standards set by standards setting organizations such as the IETF. To the extent any of our patents are considered " standards essential patents, " in some cases we may be required to license such patents to our competitors on reasonable and non- discriminatory terms or otherwise be limited in our ability to assert such patents. We also license externally developed technology that is used in some of our products and services to perform key functions. These externally developed technology licenses may not continue to be available to us on commercially reasonable terms or at all. The loss of, or our inability to obtain or maintain, any of these technology licenses could hinder or increase the cost of our services, launching new products and services, entering into new markets and / or otherwise harm our business. Some of the software and protocols used in our business are in the public domain or may otherwise become publicly available, which means that such software and protocols are or may become equally available to our competitors. We rely on the strength of our Verisign brand to help differentiate our products. Dilution of the strength of our brand could harm our business. We are at risk that we will be unable to fully register, build equity in, or enforce the Verisign logo in all markets where Verisign products and services are sold.