July 17, 2018

Fiona Alexander
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4706
Washington, D.C. 20230

Submitted via email to: iipp2018@ntia.doc.gov

RE: International Internet Policy Priorities [Docket No. 180124068-8068-01]

BSA | The Software Alliance (BSA) welcomes this opportunity to provide comments to the National Telecommunications and Information Administration (NTIA) in response to its Notice of Inquiry (NOI) on International Internet Policy Priorities.[1] BSA is the leading advocate for the global software industry before governments and in the international marketplace.[2] The software industry contributes more than $1.1 trillion to U.S. GDP and supports 10.5 million U.S. jobs.[3] Software, combined with the more than $63 billion that the industry invests annually in research and development, serves as a powerful catalyst for U.S. economic growth, making companies more competitive and the economy more robust.

As the NOI notes, the NTIA was established to advocate for policies that enable the United States to "tak[e] advantage of continued investments" in IT.[4] Its mission includes "promoting the benefits of technological development," "fostering national safety and security, economic prosperity, and the delivery of critical services" through information and communications technologies (ICT) and networks, and "facilitating and contributing to the

[1] 83 Fed. Reg. 26036 (June 5, 2018) [hereinafter "NOI"].

[2] BSA's members include Adobe, ANSYS, Apple, Autodesk, Bentley Systems, Box, CA Technologies, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Microsoft, Okta, Oracle, salesforce.com, SAS Institute, Siemens, PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro, and Workday.

[3] *See* Software.org: The BSA Foundation, *The Growing $1 Trillion Economic Impact of Software*, at 5 (Sept. 2017), available at https://software.org/wp-content/uploads/2017_Software_Economic_Impact_Report.pdf.

[4] NOI, *supra* n. 1, at 26036 (citing 47 U.S.C. 901(b)).

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

full development of competition, efficiency, and the free flow of commerce in domestic and international telecommunications markets."[5]

The Internet itself reflects the importance of this mission. As Assistant Secretary for Information and Communications and NTIA Administrator David Redl recently noted, "the Internet has transformed the American economy, creating a digital economy representing nearly 6.5 percent of the nation's GDP, or $1.2 trillion."[6] Most software products and services that U.S. enterprises depend on today—including cloud computing platforms and services, artificial intelligence, big data analytics, the Internet of Things (IoT), and similar technologies—rely on the Internet and other information networks. These technologies help enterprises analyze immense amounts of data from many different sources and turn this information into actionable intelligence. Preserving the ability of companies to use the Internet and related technologies for commerce, including to transfer data freely across borders, is critical to the competitiveness of U.S. industry and the growth of the U.S. and global economies.

We therefore welcome the NOI's focus on the international dimensions of U.S. Internet policy. Our comments below respond to points I ("The Free Flow of Information and Jurisdiction"), III ("Privacy and Security"), and IV ("Emerging Technologies and Trends") of the NOI.

I. The Free Flow of Information and Jurisdiction

Increasingly, the U.S. and global economies are fueled by data. By 2021, global IP traffic is expected to reach 3.3 trillion gigabytes of data annually—nearly three times the traffic of 2016.[7] This growth is being driven in part by a massive increase in Internet-connected devices, whose total number will exceed three times the global population by 2021.[8] Decreasing costs for data storage, increasingly powerful networks, and new innovations in capturing and analyzing all of this data are driving transformational change across the economy, making businesses more agile and competitive, governments more responsive, and empowering workers and consumers.

These changes are having profound impacts on U.S. trade and economic growth. According to the U.S. International Trade Commission (ITC), digital trade was responsible for an estimated increase in U.S. gross domestic product of 3.4 percent to 4.8 percent in 2011, and

---

[5] 47 U.S.C. § 901(c) (1)-(3).

[6] *Remarks of Assistant Secretary Redl at the National Security Telecommunications Advisory Committee (NSTAC) Meeting* (May 17, 2018), available at https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-national-security-telecommunications-advisory.

[7] Cisco, *The Zettabyte Era: Trends and Analysis* (June 7, 2017), available at https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html.

[8] *Id.*

for the creation of up to 2.4 million jobs.[9] In 2016, U.S. exports of ICT-enabled services (excluding digital goods) was $404 billion, while global e-commerce reached $27.7 trillion, up from $19.3 trillion in 2012.[10] Economists predict that making better use of data could lead to a "data dividend" of $1.6 trillion in the coming years and that data-enabled efficiency gains could add almost $15 trillion to global GDP by 2030.[11]

In order to realize these benefits, it is essential that data can move freely across borders. Cross-border data flows benefit people everywhere and are vital to nearly every sector of the economy—for example:[12]

- Healthcare. Hospitals and other healthcare organizations often need to transfer personal data across borders for use in clinical support software, which analyzes electronic health records, health insurance claims and data sets to help caregivers improve the effectiveness of medical treatments and reduce risks.

- Security and public safety. For many multinational companies, the ability to collect and analyze data across the entire organization is essential to maintaining robust cybersecurity and to detect and prevent fraud. Sharing information across borders also helps law enforcement combat crimes, and can help governments coordinate responses to natural disasters more rapidly and effectively.

- E-commerce. Companies engaged in e-commerce regularly need to transfer personal and other data across borders to keep track of their customers' orders and product supplies. Many online retailers rely upon third-party retailers to sell their products, and therefore likewise may need to move both customer and vendor data across borders.

- Global business. Businesses that operate internationally increasingly use data analytics to reach more customers, improve customer experiences, and work more efficiently. This requires them to pool large amounts of data from databases and servers around the world.

Despite these clear benefits, U.S. companies today face significant barriers to transferring data across borders. These barriers range from data localization requirements to unreasonable constraints on the ability to transfer certain types of data across borders. Although governments often invoke privacy or national security as justifications for these

---

[9] U.S. International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 2* (2014), available at https://www.usitc.gov/publications/332/pub4485.pdf.

[10] *See* Rachel F Fefer, Shayerah Ilias Akhtar, and Wayne M. Morrison, *Digital Trade and U.S. Trade Policy*, at 4- 6, CONGRESSIONAL RESEARCH SERVICE (May 11, 2018) (citing Bureau of Economic Research data), available at https://fas.org/sgp/crs/misc/R44565.pdf.

[11] *See* BSA, *What's the Big Deal With Data?* 14 (Oct. 2015), at http://data.bsa.org/wp-content/uploads/2015/10/bsadatastudy_en.pdf.

[12] *See* BSA, *Cross-Border Data Flows*, available at http://www.bsa.org/~/media/Files/Policy/BSA_2017CrossBorderDataFlows.

barriers, too often they have significant trade-distorting and protectionist effects, in part because the means chosen are significantly more trade-restrictive than necessary to achieve any legitimate public policy goal.

In several recent studies, the ITC has undertaken to catalogue many of these barriers.[13] Despite substantial attention to the problem, however, it persists in many parts of the world. In our recent Special 301 Submission to the United States Trade Representative, we cataloged a number of the most damaging data-related trade barriers.[14] Vietnam, for instance, imposes server localization requirements and restrictions on cross-border data transfers that inhibit the ability of BSA members and other U.S. companies to provide digital services in the country.[15] Taiwan does not allow government agencies to procure cloud services from companies that store data outside the country.[16] Other barriers to transferring data across borders can be found in other jurisdictions as well, including Brazil, China, India, Indonesia, Korea, and Nigeria.[17]

We urge the NTIA to promote policies, both within the Administration and with our trading partners, aimed at eliminating these and other unjustified restrictions on the flow of information across borders. We particularly encourage the Administration to engage bilaterally and multilaterally with other governments on these issues. Barriers to cross-border data flows, including requirements to store data in local facilities, undermine the enormous economic and social benefits that can accrue from data analysis and innovation. Removing restrictions on cross-border data transfers and related barriers should therefore be a top priority for the U.S. Government.

In pursuing this goal, we urge the NTIA to promote certain key principles:

- First, the Administration should seek commitments from foreign governments to refrain from adopting rules that force U.S. enterprises to store data locally, or that otherwise limit their ability to transfer data across borders. We recognize that governments often adopt measures to promote legitimate public policy goals, such as privacy or national security, and that such measures may at times constrain the ability to transfer certain types of data across borders. To ensure that these measures are not protectionist, however, they must not discriminate against foreign suppliers or constitute a disguised restriction on trade, and in all events must be no more trade restrictive than necessary to achieve the specific objective at issue.

---

[13] *See, e.g.*, ITC, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions* (Aug. 2017), available at https://www.usitc.gov/publications/332/pub4716_0.pdf; ITC, *supra* n. 9.

[14] *See* BSA, *Special 301 Submission*, at 28 (Feb. 8, 2018), available at http://www.bsa.org/~/media/Files/Policy/Trade/BSA2018Special301.pdf.

[15] *Id.* at 28.

[16] *Id.* at 3.

[17] *Id.* at 2.

- Second, the Administration should urge foreign governments, when regulating activities relating to lawful online communications or commerce, to respect the limits of their jurisdiction and give due regard to U.S. interests under established principles of international comity. The inherently global nature of the Internet significantly increases the risk that businesses will face conflicting legal obligations--*e.g.*, to store digital data in one jurisdiction when it is needed in another, or to remove online data globally even when it is legally protected elsewhere. To minimize such conflicts, governments should proceed cautiously when regulating online activities and adopt (or maintain) a strong presumption against the extraterritorial application of their laws.

In BSA's view, trade agreements offer the most promising avenue to advance these principles and promote rules safeguarding the freedom to transfer data across borders. We applaud the Administration's efforts to modernize NAFTA by establishing gold-standard rules for an integrated North American digital economy. Binding obligations by all Parties will facilitate cross-border data flows across the region and limit the ability of our trading partners to impose data localization requirements. High-standard rules in NAFTA also will serve as a model for other governments and as a template for U.S. trade agreements with other countries, including in Asia and elsewhere.

Another key priority is to ensure that trans-Atlantic trade continues to thrive. We urge the Administration to continue its work with the European Commission on the EU-U.S. Privacy Shield, which will undergo its second annual review this summer. We also encourage the NTIA to work with others in the Administration to explore further opportunities to key trading partners to facilitate data-driven economic growth and protect against barriers to digital trade.

II. Privacy and Security

Consumers, businesses, and governments everywhere are moving online. This shift to a digital, data-driven economy is transforming commerce and society, providing enormous benefits to people and governments and helping U.S. businesses enter new markets and compete more effectively. Digital technologies are driving efficiency and productivity gains in every industry and fueling innovation at an unprecedented rate.

The public's embrace of the digital economy, however, cannot be taken for granted. Ensuring that customers have faith in the security and privacy of their personal data is vital to gaining their trust in digital services and technologies. Losing that trust will lead consumers to reject these technologies and forego all of the benefits they offer.

Unfortunately, the ongoing drumbeat of high-profile data breaches, malware attacks, and other security and privacy incidents threatens to undermine consumer trust in the digital economy--while also imposing significant costs on governments and industry. Experts predict that cybercrime alone could impose costs of up to $6 trillion globally by 2021--

equivalent to nearly one third of current U.S. GDP.[18] Indeed, cybercrime is the fastest-growing sector of crime in the United States, and attacks are increasing in size, sophistication, and cost.[19]

One important way in which governments can promote strong cybersecurity and privacy, and thereby strengthen consumer trust, is to remove impediments to cross-border data transfers (as discussed in Part I). The ability to transfer data freely across borders is necessary to reap the full benefits of cloud computing and similar distributed computing architectures, which can compartmentalize datasets and make it easier to prevent a breach in one location from infecting the full dataset.[20] Access to data held abroad also can help companies more quickly detect and isolate attacks in their networks, and to maintain copies of particularly sensitive data in secure locations.[21] In short, preserving firms' ability to transfer data across borders will facilitate their ability to strengthen cybersecurity and improve their resilience against attacks.

More broadly, addressing cybersecurity threats, and the risks they pose to privacy and data protection, requires a multi-faceted and holistic approach that involves industry, governments, and consumers.

A. Industry Efforts

BSA members invest heavily in helping protect their customers, and society more broadly, against cybersecurity threats. For instance, BSA members are industry leaders in the development and adoption of security-by-design principles and secure software development lifecycle processes. Broad adherence to these practices is vital to reducing the vulnerabilities that malicious actors exploit in attacks, including those leading to the theft or disclosure of personal or other sensitive information. We urge NTIA to work with others in the Administration to encourage broader adoption of these practices, including by promoting their use with software developers and organizations that evaluate software suppliers.[22]

BSA members are also committed to implementing world-class cybersecurity practices and privacy programs. Many BSA members, for instance, are certified under the EU-U.S. Privacy Shield, which combines robust privacy commitments with mechanisms to facilitate personal data transfers between the EU and United States. BSA members have also led efforts to

---

[18] *See Cybercrime Damages $6 Trillion By 2021*, CYBERSECURITY VENTURES, available at https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

[19] *Id.*

[20] *See* BSA, *supra* n. 12.

[21] *Id.*

[22] BSA recently proposed that future versions of the NIST *Framework for Improving Critical Infrastructure Cybersecurity* include such guidance for organizations evaluating software suppliers. *See* BSA, *BSA International Cybersecurity Policy Framework*, at 15, available at https://bsacybersecurity.bsa.org/wp-content/uploads/2018/04/BSA_cybersecurity-policy.pdf.

develop international standards in this area, such as the ISO 27000 family of information security management standards that form the basis of the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.

Many other industry-led cybersecurity efforts are underway or under consideration. For instance, the Departments of Commerce and Homeland Security recently issued a report proposing a voluntary security labeling scheme for IoT products.[23] As BSA has noted separately, we think such proposals are promising, provided they are truly market-driven, that certifications are flexible and outcomes-oriented, that approaches are aligned so that consumers are not confused by differing labels or certifications, and assessment and/or certification processes are transparent, and that labels and other tools are sufficiently flexible and nuanced to meaningfully capture security considerations across a wide range of software products.[24]

B. Joint Industry-Government Efforts

A second essential element in helping protect U.S. consumers and businesses against cybersecurity threats is robust partnership between the public and private sectors. In particular, BSA strongly supports a robust partnership of government and industry to:

- Promote a secure software ecosystem by creating industry benchmarks, developing tools to understand critical information, and strengthening security research and vulnerability disclosure;

- Strengthen government's approach to cybersecurity by modernizing government IT, harmonizing federal cybersecurity regulations, and incentivizing adoption of the NIST framework;

- Pursue international consensus for cybersecurity action by supporting international standards development as well as adopting and streamlining international security laws;

- Develop a 21st century cybersecurity workforce by increasing access to computer science education and opening new paths to cybersecurity careers; and

[23] *See A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*, at 44-45 (May 22, 2018), available at https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.

[24] *See BSA Letter to NTIA Re: Promoting Stakeholder Action Against Botnets and Other Automated Threats [Docket No. 180103005-8005-01]*, at 4 (Feb. 12, 2018), available at http://www.bsa.org/~/media/Files/Policy/Security/Letters/02122018BSA_NTIABotnetReportComments.pdf.

- Advance cybersecurity through digital transformation by leveraging the potential of emerging technologies and forging innovative partnerships to combat emerging risks.[25]

NTIA is well positioned to advocate for such policies within the Administration, and we look forward to opportunities to work together with NTIA to advance these goals.

C. International Engagement

As the NOI recognizes,[26] an effective response to cybersecurity threats must take into account the global nature of these threats. For instance, botnets often involve networks of infected machines located in multiple countries, with command-and-control nodes often located outside the jurisdiction of U.S. law enforcement. Therefore, international collaboration is vital to addressing these threats.

Consistent with NTIA's mission and the recent joint Department of Commerce and Department of Homeland Security Report to the President on *Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*,[27] BSA encourages the Administration to engage actively with key U.S. allies and trading partners to develop coordinated and effective responses to cybersecurity threats. In doing so, we encourage the Administration to promote cybersecurity policies that are: (1) aligned with internationally recognized technical standards; (2) risk-based, outcome-focused, and technology neutral; (3) rely on market-driven mechanisms where possible; (4) flexible and adaptable in order to encourage innovation; (5) rooted in public-private collaboration; and (6) oriented to protect privacy. BSA recently released an International Cybersecurity Policy Framework that articulates and builds on these concepts; we believe it could be a useful reference guide as the United States engages with other governments on these issues.[28]

BSA encourages NTIA and others in the Administration to continue bilateral engagements with their international counterparts, particularly in Asia, as these jurisdictions consider adopting new or revised data protection and cybersecurity frameworks, in particular to ensure that these frameworks promote privacy and security without impeding responsible

---

[25] *See* BSA, *A Cybersecurity Agenda for the Connected Age*, available at https://bsacybersecurity.bsa.org/wp-content/uploads/2018/04/BSA_CybersecurityAgenda.pdf.

[26] *See* NOI, *supra* n. 1, at 26037.

[27] *See supra* n. 23, at 49 ("The global nature of distributed threats was frequently highlighted during the process executed by Commerce and Homeland Security. Stakeholders highlighted the importance of international standards, policies, and best practices in promoting international participation and collaboration. By continuing to advocate for industry-led approaches and by actively participating in development of voluntary, consensus-based international standards, the federal government can contribute to pragmatic and effective outcome-based standards that meet the needs of all stakeholders. The federal government is also uniquely positioned to lead the international engagement required to establish broadly accepted policies and best practices and will enhance coordination with stakeholders on these efforts.").

[28] *See* BSA, *supra* n. 22.

innovation or technology use. The Administration should likewise engage with trading partners, such as the European Union, that are pursuing cybersecurity certification regimes to ensure they are developed in close, open consultation with stakeholders and are aligned with international, consensus-based standards to the greatest extent possible.

At the multilateral level, we encourage the Administration to support the continued development of robust mechanisms to facilitate cross-border data transfers, such as the APEC Cross Border Privacy Rules,[29] and to promote interoperability between the privacy and data protection regimes of various regions, including potentially with the European Union via certification programs. BSA also supports the fact-finding and analysis currently underway by the OECD's Working Party on Security and Privacy in the Digital Economy.[30] We appreciate the United States' leadership in the OECD and urge the Administration to continue working to ensure that the Organization's policy recommendations are evidence based, aligned with U.S. interest, and promote innovation.

Finally, we encourage NTIA to continue working in coordination with others in the Administration to find a resolution to ensure that both law enforcement personnel and private sector security professionals can access the WHOIS database. When a security analyst identifies a cyberattack emanating from a specific domain, the WHOIS database enables her to correlate the malicious domain with others that are likely to be owned or operated by the same criminal entity. These correlations can be used to preemptively block future attacks and help investigators uncover the identity of malicious actors.[31] Access to the WHOIS database is now threatened, however, due to a narrow interpretation of the EU's General Data Protection Regulation.[32] As Associate Deputy Attorney General Sujit Raman recently noted, such an outcome creates significant public safety risks. BSA therefore encourages the Administration to engage bilaterally and multilaterally to ensure security personnel can access the WHOIS database for purposes preventing malicious online activity.

III. Emerging Technologies and Trends

We welcome the NOI's focus on emerging technology trends and their implications for the Administration's international policy priorities. Innovations in software are propelling the development of many new technologies that offer great promise to improve lives, help solve important social challenges, and generate substantial economic growth in the years ahead.

---

[29] *See, e.g.*, *APEC Cross Border Privacy Rules System*, available at http://www.cbprs.org/.

[30] *See Working Party on Security and Privacy in the Digital Economy*, available at http://www.oecd.org/sti/ieconomy/workingpartyonsecurityandprivacyinthedigitaleconomyspde.htm.

[31] *See* Caleb Barlow, *WHOIS Behind Cyberattacks? Under GDPR, We May Not Know*, IBM Security Intelligence (May 8, 2018), available at https://securityintelligence.com/whois-behind-cyberattacks-under-gdpr-we-may-not-know.

[32] *See Remarks of Assistant Secretary Redl at the National Security Telecommunications Advisory Committee (NSTAC) Meeting* (May 17, 2018), available at https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-national-security-telecommunications-advisory.

One broad category of such technologies—and which is of particular interest given its potentially wide-ranging applications across virtually the entire economy and society—is artificial intelligence (AI). AI is at its core is a technology that augments human intelligence, helping people make better-informed decisions by identifying relationships, patterns, and trends in data that would be imperceptible to humans.[33] AI systems are "trained" by ingesting large volumes of data, and the resulting algorithms are then applied to new sets of data to provide insights, make predictions, and help inform and guide action.

AI solutions are already being applied across the economy to improve lives and benefit society. Although the potential applications of AI are almost endless, notable examples include AI solutions that improve the delivery of healthcare and quality of life, bolster security and better protect privacy, help create smarter and safer cities through infrastructure improvements, improve access to and quality of education, and enhance agricultural practices.[34] More broadly, AI has the potential to generate substantial economic growth and help governments provide better and more responsive government services while also addressing some of the world's most pressing societal challenges.

Given the transformational potential of AI, governments around the world are beginning to focus on developing policy frameworks to address both the opportunities and possible risks associated with certain applications of AI. BSA encourages the NTIA to work in partnership with others in the Administration to ensure that the United States maintains a leading voice in the development of international policies to guide the future growth and development of AI.

BSA recently proposed a policy framework that is intended to help governments promote the responsible development and use of AI.[35] Specifically, we urge governments to support policies that: (1) establish confidence and trust in AI systems;[36] (2) encourage data innovation (e.g., ensuring data can move freely across borders, providing access to government data, and supporting value-added data services);[37] (3) strengthen cybersecurity and privacy protections; (4) promote investments in research and development; and, (5) provide the workforce with access to training and educational opportunities to prepare them for the jobs of the future.

---

[33] *See* BSA, *Spurring AI Innovation With Sound Data Policy* (May 2018), available at http://www.bsa.org/~/media/Files/Policy/BSA_2018_AI_DataPolicy.pdf.

[34] *See* BSA, *Artificial Intelligence in Every Sector* (May 2018), available at http://www.bsa.org/~/media/Files/Policy/BSA_2018_AI_Examples.pdf.

[35] *See* BSA,*BSA AI Policy Overview* (May 2018), available at www.bsa.org/~/media/Files/Policy/BSA_2018_AI_PolicyOverview.pdf.

[36] *See* BSA, *Building Confidence & Trust in Artificial Intelligence Systems* (May 2018), available at https://ai.bsa.org/wp-content/uploads/2018/05/BSA_2018_AI_Accountability.pdf.

[37] *See* BSA, *Spurring AI Innovation With Sound Data Policy* (May 2018), available at https://ai.bsa.org/wp-content/uploads/2018/05/BSA_2018_AI_DataPolicy.pdf.

We note that these proposed policies align to a substantial degree with the G7 Innovation Ministers' Statement on Artificial Intelligence agreed in Montreal, Quebec in March 2018.[38] We appreciate the Administration's work on this issue, including with regard to the Common Vision for the Future of Artificial Intelligence agreed at the G7 2018 meeting in Charlevoix, Canada.[39]

IV. Conclusion

We strongly support the NTIA's decision to seek stakeholder feedback on the Administration's international Internet policy priorities, and we appreciate the opportunity to provide our perspectives on this critically important issue. We would be pleased to provide further information as needed and to answer any questions the NTIA might have.

* * * * *

Thank you again for the opportunity to share our views on these important issues.

Sincerely,

Christian Troncoso
Director, Policy

[38] *See Annex B: G7 Innovation Ministers' Statement on Artificial Intelligence* (March 2018), available at https://g7.gc.ca/en/g7-presidency/themes/preparing-jobs-future/g7-ministerial-meeting/chairs-summary/annex-b/.

[39] *See Common Vision for the Future of Artificial Intelligence* (June 2018), available at https://g7.gc.ca/wp-content/uploads/2018/06/FutureArtificialIntelligence.pdf.

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org