August 26, 2020

The Honorable Adam Smith
Chairman
House Armed Services Committee
2216 Rayburn House Office Building
Washington, DC 20515

The Honorable Mac Thornberry
Ranking Member
House Armed Services Committee
2216 Rayburn House Office Building
Washington, DC 20515

Dear Chairmen Smith and Ranking Member Thornberry:

BSA | The Software Alliance is grateful for your leadership on the *Fiscal Year 2021 National Defense Authorization Act* (FY21 NDAA). As conferees work to develop a final version of the bill, we write to you regarding several provisions under consideration that would impact the global software industry.

BSA[1] is the leading trade association representing the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, developing cutting-edge solutions in use across the range of information technology (IT) platforms, and are global leaders in advancing best practices for developing quality, secure, trustworthy software. Earlier this year, we wrote you about our priorities for this year's legislation to advance cybersecurity, driving agile and meaningful innovation, and harness emerging technologies, and we are grateful that you addressed many of these priorities in the legislation. As the conference committee proceeds, we urge your attention to these and other priorities, addressed below.

Artificial Intelligence

BSA's members have long been supportive of legislative efforts that seek to secure U.S. leadership in the field of artificial intelligence. To that end, we strongly support the National Artificial Intelligence Act – included in the text of Division E of the House NDAA – which establishes a federal initiative to coordinate federal investments in R&D and facilitate new public-private partnerships that will accelerate the development of cutting-edge AI. Critically, the National Artificial Intelligence Act also recognizes that US leadership in AI will require forward-thinking approaches for ensuring that the technology is developed in trustworthy and accountable ways. To that end, the legislation includes an

[1] BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, IBM, Informatica, Intel, Microsoft, Okta, Oracle, PTC, salesforce.com, ServiceNow, Siemens PLM Software, Sitecore, Slack, Splunk, Trimble Solutions Corporation, The MathWorks, Trend Micro, Twilio, and Workday.

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

important provision (Section 5301(b)) that directs NIST to begin developing a risk management framework for artificial intelligence. Given its considerable experience developing lifecycle risk management frameworks for cybersecurity and privacy, NIST is well-positioned to play a leading role in the development of a framework for AI in close collaboration with stakeholders. Importantly, a NIST AI framework would also send a powerful signal that would help inform US trading partners that are currently considering their own policy approaches for AI. A NIST-backed AI framework can therefore help shape the global debate around AI governance in ways that will inure to the benefit of the United States. **We urge you to include this provision in the final version of the FY21 bill.**

Supply Chain Security

BSA shares the Committee's goal of securing supply chains against malicious threats and inadvertent risks and appreciates its ongoing efforts to improve the Department's supply chain risk management. House and Senate versions of the FY21 NDAA include several supply chain proposals of note. In our previous letter, BSA urged the Committee to evaluate such proposals against the following principles:

- Supply chain policies should embrace internationally recognized, industry driven standards for security throughout the digital supply chain.
- Supply chain policies should be rooted in risk management approaches that prioritize security measures based on the most relevant and potentially impactful risks.
- Supply chain policies should be transparent to the public, with specific actions notified to impacted stakeholders, and should establish meaningful mechanisms for resolving disputes.
- Supply chain policies should be enforceable, for example by establishing supply chain risk management responsibilities in vendor contracts.
- Supply chain policies should be collaborative, embracing public-private partnership, information-sharing, and operational cooperation.

As conferees consider supply chain proposals, we wish to reemphasize these principles.

With 5G supply chains of increasing concern, BSA has advocated for investment in innovative software solutions to supply chain challenges, such as virtualized Radio Access Network (RAN) technology, which would replace hardware-centric RAN with software to enable greater diversity and competitiveness in the supply chain while improving performance and lowering cost. We have also advocated for open standards and interfaces, as represented in open RAN initiatives. We were pleased to see the Senate include two measures to advance virtualized RAN and open RAN development: Section 233, which would authorize the Department to carry out a virtualized RAN demonstration project, and Section 1092, which would establish grant funding to support virtualized RAN and open RAN development and deployment. We strongly support these efforts, which represent thoughtful and innovative approaches to improving supply chain risk management that are fully aligned with BSA's principles. **We urge you to include Section 233 and Section 1092 in the final version of the FY21 bill. Furthermore, given the importance of development alternatives to improve competition among providers of RAN technologies, we urge you to restore funding authorizations in the provision to the amounts included in the *USA Telecommunications Act* originally introduced by Senators Warner and Burr.**

In Section 889 of the Fiscal Year 2019 NDAA, Congress sought to address supply chain concerns relating to Huawei, ZTE, and Chinese video technology companies, and the Department just published an interim rule implementing this section. As you know, the technology industry – while sharing the

goals of the legislation – has been concerned that its broad scope will create implementation challenges and, indeed, the interim rule deepens this concern. Lack of clarity about the rule's scope and questions about the feasibility of implementation in certain circumstances demonstrate the complexity and difficulty of the legislation's implementation. For that reason, BSA was pleased to see Section 828 of the House legislation, which expresses the sense of Congress that this important legislation should be implemented in a deliberate manner. We support this statement and **would urge you to expand it to require a delay in implementation while the questions discussed above are further addressed.**

As the above principles articulate, BSA believes supply chain policies should be based on risk management and internationally recognized standards; for that reason, BSA has opposed measures to block transactions or ban vendors simply due to their national origin, because such measures fail to evaluate and prioritize risk. They also invite reciprocal policies from other nations that could harm U.S. industry. For that reason, BSA has substantial concerns about requirements in both House (Section 826) and Senate (Section 808) bills pertaining to printed circuit boards. Printed circuit boards are used in nearly all electronic products, and therefore are critical to support the operation of software products and services, including cloud services. The restrictions in these provisions appear arbitrary and out of step with a risk-based, internationally interoperable approach to supply chain security that benefits both government and industry stakeholders. **We urge you to reconsider these provisions. Given that the Department already enjoys wide latitude to intervene in acquisitions on the basis of supply chain threats, we believe an appropriate solution would be to direct the Department to apply such authorities – in line with a careful analysis and prioritization of risk – to printed circuit boards.**

Like printed circuit boards, semiconductors represent a critical dependency for the software industry, supporting operations of software products and services, including cloud services. Both the House and Senate passed amendments, offered by Rep. Doris Matsui and Sen. John Cornyn, respectively, to establish incentives for the domestic production of semiconductors. Given supply chain concerns about semiconductors, these amendments embody a common-sense approach that is fully consistent with BSA's supply chain principles. **We support these amendments and urge their inclusion in the final legislation.**

Finally, we note two supply chain concerns that, while not significantly addressed in the House and Senate versions of the NDAA, remain priorities for the software industry: the Department's development of the Cybersecurity Maturity Model Certification (CMMC) program, and its implementation of provisions relating to source code reviews of software acquired by the Pentagon (Sections 1654 and 1655 of the FY 2019 NDAA). **We urge the Committee to address these ongoing issues through rigorous oversight to guide DoD implementation in a manner that is practically feasible, rooted in risk management, transparent, and non-duplicative.**

Software Acquisition and Security

In our previous letter, we noted that BSA is eager to see the committees continue their work to improve the Department's ability to access the most innovative, secure software available, and we are pleased to see this recommendation addressed.

Section 882 of the Senate bill would require software vendors to describe their secure development lifecycle and vulnerability management practices when competing for DoD software acquisitions. We

applaud this effort to incentivize secure software development. BSA's members are the world's leading practitioners of secure software development and pioneered the secure development lifecycle; widespread adoption of these practices will substantially improve both the quality and security of DoD's digital infrastructure. **We support the inclusion of Section 882 in the final bill and would welcome the opportunity to work with the Committee to further refine the text.**

Security cannot be reduced to a single point in time; it must be maintained throughout a product's lifecycle. We believe Section 882 could be improved by requiring vendors to maintain accurate information about secure development lifecycle and vulnerability management practices throughout a contract. In addition, the provision should provide resource to vendors seeking to describe such practices as a way of standardizing submissions and the Department's evaluation of those submissions. We recommend NIST's recently published white paper outlining a "Secure Software Development Framework" (SSDF) and BSA's own *Framework for Secure Software* as two leading resources to help vendors describe their practices in ways that address industry standards and best practices across the most critical security outcomes.

Software services also play a critical role in securing sensitive data and networks, and security orchestration technologies are often at the cutting edge in this regard. BSA strongly supports the Senate's authorization (Section 1618) of a pilot program on cybersecurity capability metrics, which would include an assessment of security orchestration technologies. We believe broader use of security orchestration tools within the defense enterprise could pay enormous dividends in improving the accuracy and efficiency of incident response. **We urge you to include Section 1618 in the final version of the FY21 bill.**

Cyberspace Solarium Commission Recommendations

Previously, BSA called upon the Committee to adopt the recommendations of the Cyberspace Solarium Commission to the greatest extent possible, and we were pleased to see a number of the Commission's proposals included. In particular, BSA endorsed Rep. Jim Langevin's proposal to establish a National Cyber Director within the Executive Office of the President, and we were grateful that this proposal was adopted. **We urge conferees to maintain this provision in the final bill.**

One recommendation that we are concerned may not be ready for inclusion in the final bill is a proposal, offered as an amendment by Rep. Cedric Richmond, to establish a mandatory cyber incident reporting regime for U.S. critical infrastructure. Cyber incident reporting can be a valuable way to improve the government's timely awareness of emerging cyber threats; however, it also entails a complex process that differs across various organizations and their distinctive cybersecurity programs. Reporting mandates can derail efforts to contain and respond to cyber incidents and can cause confusion by leading to early reports that prove inaccurate as more information is gathered. The provision's mandated 72-hour reporting deadline is particularly problematic in this regard. BSA strongly supports efforts to expand cyber incident reporting, in critical infrastructure and beyond, but is concerned that this particular provision is not fully developed and could have unintended consequences. **We recommend that you refrain from including this provision in the final legislation.**

Cybersecurity Workforce

BSA has long advocated for government leadership in building a cybersecurity workforce for the 21st century and has commended the Committee for its sustained efforts to support such a goal. This

year's NDAA includes a number of important workforce provisions. BSA would like to highlight three priorities in particular. First, Sec. 511 of the House bill would establish a grant program to support science, technology, engineering, and mathematics (STEM) education in the Junior Reserve Officers' Training Corps. This proposal represents an excellent opportunity to invest early in building tomorrow's cybersecurity workforce. Likewise, Subtitle D of the Senate NDAA includes two amendments sponsored by Senator Wicker, based on S. 2775 and S. 3712, to improve the National Initiative for Cybersecurity Education and establish national cybersecurity grand challenges to seek high-priority cybersecurity breakthroughs. **BSA supports each of these provisions and urges their inclusion in the final bill.**

Digital Modernization

Software brings manifold opportunities for organizations to improve the efficiency, accuracy, and speed of their business practices, and the Department of Defense, as one of the world's largest organizations, stands to benefit particularly from these opportunities. In 2018, Congress passed P.L. 115-336, the *21st Century Integrated Digital Experience Act* ("21st Century IDEA"), which embraces government agency digital modernization through expanding use of electronic signatures and digital forms, making websites more accessible, digitizing citizen services, and other measures. DoD has been slow to implement the Act, and **BSA is grateful to both committees for including committee report language directing the Department to implement the legislation**. We look forward to continuing to work with you to enable the Pentagon to reap the full benefits of digital modernization.

We would welcome the opportunity to work with you and your staff to address these priorities in the final version of the FY21 NDAA. Thank you for your leadership, and we look forward to working with you.

Sincerely,

Craig Albright
VP, Legislative Strategy

August 26, 2020

The Honorable James Inhofe
Chairman
Senate Armed Services Committee
228 Russell Senate Office Building
Washington, DC 20510

The Honorable Jack Reed
Ranking Member
Senate Armed Services Committee
228 Russell Senate Office Building
Washington, DC 20510

Dear Chairmen Inhofe and Ranking Member Reed:

BSA | The Software Alliance is grateful for your leadership on the *Fiscal Year 2021 National Defense Authorization Act* (FY21 NDAA). As conferees work to develop a final version of the bill, we write to you regarding several provisions under consideration that would impact the global software industry.

BSA[1] is the leading trade association representing the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, developing cutting-edge solutions in use across the range of information technology (IT) platforms, and are global leaders in advancing best practices for developing quality, secure, trustworthy software. Earlier this year, we wrote you about our priorities for this year's legislation to advance cybersecurity, driving agile and meaningful innovation, and harness emerging technologies, and we are grateful that you addressed many of these priorities in the legislation. As the conference committee proceeds, we urge your attention to these and other priorities, addressed below.

Artificial Intelligence

BSA's members have long been supportive of legislative efforts that seek to secure U.S. leadership in the field of artificial intelligence. To that end, we strongly support the National Artificial Intelligence Act – included in the text of Division E of the House NDAA – which establishes a federal initiative to coordinate federal investments in R&D and facilitate new public-private partnerships that will accelerate the development of cutting-edge AI. Critically, the National Artificial Intelligence Act also recognizes that US leadership in AI will require forward-thinking approaches for ensuring that the technology is developed in trustworthy and accountable ways. To that end, the legislation includes an

[1] BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, IBM, Informatica, Intel, Microsoft, Okta, Oracle, PTC, salesforce.com, ServiceNow, Siemens PLM Software, Sitecore, Slack, Splunk, Trimble Solutions Corporation, The MathWorks, Trend Micro, Twilio, and Workday.

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

important provision (Section 5301(b)) that directs NIST to begin developing a risk management framework for artificial intelligence. Given its considerable experience developing lifecycle risk management frameworks for cybersecurity and privacy, NIST is well-positioned to play a leading role in the development of a framework for AI in close collaboration with stakeholders. Importantly, a NIST AI framework would also send a powerful signal that would help inform US trading partners that are currently considering their own policy approaches for AI. A NIST-backed AI framework can therefore help shape the global debate around AI governance in ways that will inure to the benefit of the United States. **We urge you to include this provision in the final version of the FY21 bill.**

Supply Chain Security

BSA shares the Committee's goal of securing supply chains against malicious threats and inadvertent risks and appreciates its ongoing efforts to improve the Department's supply chain risk management. House and Senate versions of the FY21 NDAA include several supply chain proposals of note. In our previous letter, BSA urged the Committee to evaluate such proposals against the following principles:

- Supply chain policies should embrace internationally recognized, industry driven standards for security throughout the digital supply chain.
- Supply chain policies should be rooted in risk management approaches that prioritize security measures based on the most relevant and potentially impactful risks.
- Supply chain policies should be transparent to the public, with specific actions notified to impacted stakeholders, and should establish meaningful mechanisms for resolving disputes.
- Supply chain policies should be enforceable, for example by establishing supply chain risk management responsibilities in vendor contracts.
- Supply chain policies should be collaborative, embracing public-private partnership, information-sharing, and operational cooperation.

As conferees consider supply chain proposals, we wish to reemphasize these principles.

With 5G supply chains of increasing concern, BSA has advocated for investment in innovative software solutions to supply chain challenges, such as virtualized Radio Access Network (RAN) technology, which would replace hardware-centric RAN with software to enable greater diversity and competitiveness in the supply chain while improving performance and lowering cost. We have also advocated for open standards and interfaces, as represented in open RAN initiatives. We were pleased to see the Senate include two measures to advance virtualized RAN and open RAN development: Section 233, which would authorize the Department to carry out a virtualized RAN demonstration project, and Section 1092, which would establish grant funding to support virtualized RAN and open RAN development and deployment. We strongly support these efforts, which represent thoughtful and innovative approaches to improving supply chain risk management that are fully aligned with BSA's principles. **We urge you to include Section 233 and Section 1092 in the final version of the FY21 bill. Furthermore, given the importance of development alternatives to improve competition among providers of RAN technologies, we urge you to restore funding authorizations in the provision to the amounts included in the *USA Telecommunications Act* originally introduced by Senators Warner and Burr.**

In Section 889 of the Fiscal Year 2019 NDAA, Congress sought to address supply chain concerns relating to Huawei, ZTE, and Chinese video technology companies, and the Department just published an interim rule implementing this section. As you know, the technology industry – while sharing the

goals of the legislation – has been concerned that its broad scope will create implementation challenges and, indeed, the interim rule deepens this concern. Lack of clarity about the rule's scope and questions about the feasibility of implementation in certain circumstances demonstrate the complexity and difficulty of the legislation's implementation. For that reason, BSA was pleased to see Section 828 of the House legislation, which expresses the sense of Congress that this important legislation should be implemented in a deliberate manner. We support this statement and **would urge you to expand it to require a delay in implementation while the questions discussed above are further addressed.**

As the above principles articulate, BSA believes supply chain policies should be based on risk management and internationally recognized standards; for that reason, BSA has opposed measures to block transactions or ban vendors simply due to their national origin, because such measures fail to evaluate and prioritize risk. They also invite reciprocal policies from other nations that could harm U.S. industry. For that reason, BSA has substantial concerns about requirements in both House (Section 826) and Senate (Section 808) bills pertaining to printed circuit boards. Printed circuit boards are used in nearly all electronic products, and therefore are critical to support the operation of software products and services, including cloud services. The restrictions in these provisions appear arbitrary and out of step with a risk-based, internationally interoperable approach to supply chain security that benefits both government and industry stakeholders. **We urge you to reconsider these provisions. Given that the Department already enjoys wide latitude to intervene in acquisitions on the basis of supply chain threats, we believe an appropriate solution would be to direct the Department to apply such authorities – in line with a careful analysis and prioritization of risk – to printed circuit boards.**

Like printed circuit boards, semiconductors represent a critical dependency for the software industry, supporting operations of software products and services, including cloud services. Both the House and Senate passed amendments, offered by Rep. Doris Matsui and Sen. John Cornyn, respectively, to establish incentives for the domestic production of semiconductors. Given supply chain concerns about semiconductors, these amendments embody a common-sense approach that is fully consistent with BSA's supply chain principles. **We support these amendments and urge their inclusion in the final legislation.**

Finally, we note two supply chain concerns that, while not significantly addressed in the House and Senate versions of the NDAA, remain priorities for the software industry: the Department's development of the Cybersecurity Maturity Model Certification (CMMC) program, and its implementation of provisions relating to source code reviews of software acquired by the Pentagon (Sections 1654 and 1655 of the FY 2019 NDAA). **We urge the Committee to address these ongoing issues through rigorous oversight to guide DoD implementation in a manner that is practically feasible, rooted in risk management, transparent, and non-duplicative.**

Software Acquisition and Security

In our previous letter, we noted that BSA is eager to see the committees continue their work to improve the Department's ability to access the most innovative, secure software available, and we are pleased to see this recommendation addressed.

Section 882 of the Senate bill would require software vendors to describe their secure development lifecycle and vulnerability management practices when competing for DoD software acquisitions. We

applaud this effort to incentivize secure software development. BSA's members are the world's leading practitioners of secure software development and pioneered the secure development lifecycle; widespread adoption of these practices will substantially improve both the quality and security of DoD's digital infrastructure. **We support the inclusion of Section 882 in the final bill and would welcome the opportunity to work with the Committee to further refine the text.**

Security cannot be reduced to a single point in time; it must be maintained throughout a product's lifecycle. We believe Section 882 could be improved by requiring vendors to maintain accurate information about secure development lifecycle and vulnerability management practices throughout a contract. In addition, the provision should provide resource to vendors seeking to describe such practices as a way of standardizing submissions and the Department's evaluation of those submissions. We recommend NIST's recently published white paper outlining a "Secure Software Development Framework" (SSDF) and BSA's own *Framework for Secure Software* as two leading resources to help vendors describe their practices in ways that address industry standards and best practices across the most critical security outcomes.

Software services also play a critical role in securing sensitive data and networks, and security orchestration technologies are often at the cutting edge in this regard. BSA strongly supports the Senate's authorization (Section 1618) of a pilot program on cybersecurity capability metrics, which would include an assessment of security orchestration technologies. We believe broader use of security orchestration tools within the defense enterprise could pay enormous dividends in improving the accuracy and efficiency of incident response. **We urge you to include Section 1618 in the final version of the FY21 bill.**

Cyberspace Solarium Commission Recommendations

Previously, BSA called upon the Committee to adopt the recommendations of the Cyberspace Solarium Commission to the greatest extent possible, and we were pleased to see a number of the Commission's proposals included. In particular, BSA endorsed Rep. Jim Langevin's proposal to establish a National Cyber Director within the Executive Office of the President, and we were grateful that this proposal was adopted. **We urge conferees to maintain this provision in the final bill.**

One recommendation that we are concerned may not be ready for inclusion in the final bill is a proposal, offered as an amendment by Rep. Cedric Richmond, to establish a mandatory cyber incident reporting regime for U.S. critical infrastructure. Cyber incident reporting can be a valuable way to improve the government's timely awareness of emerging cyber threats; however, it also entails a complex process that differs across various organizations and their distinctive cybersecurity programs. Reporting mandates can derail efforts to contain and respond to cyber incidents and can cause confusion by leading to early reports that prove inaccurate as more information is gathered. The provision's mandated 72-hour reporting deadline is particularly problematic in this regard. BSA strongly supports efforts to expand cyber incident reporting, in critical infrastructure and beyond, but is concerned that this particular provision is not fully developed and could have unintended consequences. **We recommend that you refrain from including this provision in the final legislation.**

Cybersecurity Workforce

BSA has long advocated for government leadership in building a cybersecurity workforce for the 21st century and has commended the Committee for its sustained efforts to support such a goal. This

year's NDAA includes a number of important workforce provisions. BSA would like to highlight three priorities in particular. First, Sec. 511 of the House bill would establish a grant program to support science, technology, engineering, and mathematics (STEM) education in the Junior Reserve Officers' Training Corps. This proposal represents an excellent opportunity to invest early in building tomorrow's cybersecurity workforce. Likewise, Subtitle D of the Senate NDAA includes two amendments sponsored by Senator Wicker, based on S. 2775 and S. 3712, to improve the National Initiative for Cybersecurity Education and establish national cybersecurity grand challenges to seek high-priority cybersecurity breakthroughs. **BSA supports each of these provisions and urges their inclusion in the final bill.**

Digital Modernization

Software brings manifold opportunities for organizations to improve the efficiency, accuracy, and speed of their business practices, and the Department of Defense, as one of the world's largest organizations, stands to benefit particularly from these opportunities. In 2018, Congress passed P.L. 115-336, the *21st Century Integrated Digital Experience Act* ("21st Century IDEA"), which embraces government agency digital modernization through expanding use of electronic signatures and digital forms, making websites more accessible, digitizing citizen services, and other measures. DoD has been slow to implement the Act, and **BSA is grateful to both committees for including committee report language directing the Department to implement the legislation**. We look forward to continuing to work with you to enable the Pentagon to reap the full benefits of digital modernization.

We would welcome the opportunity to work with you and your staff to address these priorities in the final version of the FY21 NDAA. Thank you for your leadership, and we look forward to working with you.

Sincerely,

Craig Albright
VP, Legislative Strategy

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