U.S. SMALL BUSINESS ADMINISTRATION
OFFICE OF ADVOCACY
REGULATION • RESEARCH • OUTREACH

June 23, 2021

VIA ELECTRONIC SUBMISSION

Dr. James Olthoff
Director
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Re: NIST Cyber Supply Chain Risk Management Practices for Systems and Organizations

Dear Director Olthoff:

The U.S. Small Business Administration's Office of Advocacy (Advocacy) submits the following comments in response to the National Institute of Standards and Technology (NIST) draft publication Cyber Supply Chain Risk Management Practices for Systems and Organizations.[1]

Advocacy appreciates NIST's efforts to make this publication more consumable but is concerned that NIST does not discuss small businesses. Advocacy recommends that NIST discuss the risk that this guidance will become a set of de facto requirements and the effect that would have on small businesses. Advocacy also recommends that NIST describe the small businesses in the cyber supply chain and how this guidance pertains to them, as well as provide summary information that small businesses can easily understand. Finally, NIST should discuss how components of this guidance relate to policies from other agencies and to some of the broader cybersecurity issues facing small businesses.

The Office of Advocacy

Congress established Advocacy under Pub. L. 94-305 to represent the views of small entities before Federal agencies and Congress. Advocacy is an independent office within the U.S. Small Business Administration (SBA); as such, the views expressed by Advocacy do not necessarily reflect the views of the SBA or the Administration.

[1] National Institute of Standards and Technology, Cyber Supply Chain Risk Management Practices for Systems and Organizations (Draft NIST Special Publication 800-161, Revision 1, April 2021), https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft.

Background

NIST is seeking comments on revisions to its 2015 cyber supply chain risk management guidance.[2] The revision updates the guidance to reflect new data and best practices, and to align its recommendations with those in other NIST guidance documents.

Advocacy's Comments on the Revised Special Publication

1. *Advocacy is concerned about the potential for recommendations in the new guidance to become de facto requirements.*

While NIST is taking important steps to address cyber supply chain risk, Advocacy is concerned that this publication may create new industry norms that businesses must adopt to remain competitive, but which are prohibitively expensive for small businesses. Although NIST frames the publication as guidance, the contents can become de facto requirements in the cyber supply chain if enough businesses or government entities use the guidance as a set of minimum standards when buying or selling software or contracting with others. The recent executive order mandating new standards for software sold to the government makes this outcome more likely.[3] A discussion of any such phenomenon following previous guidance from NIST would provide helpful insight for businesses unsure of the ramifications, particularly small businesses deciding whether they need to adopt components of the guidance to remain competitive.

2. *The guidance should describe the affected small businesses and whether recommendations are feasible based on limited resources.*

This publication does not include a thorough discussion of the number and characteristics of small businesses in the cyber supply chain. The Computer Systems Design and Related Services industry alone includes over 120,000 small businesses in just a portion of the cyber supply chain.[4] For example, Department of Defense (DOD) cybersecurity measures apply to over 300,000 businesses in the DOD supply chain.[5] An estimate of the number and a description of affected small businesses in the cyber supply chain would clarify which small businesses might be impacted by the new standards, and the resources necessary for them to comply.

Advocacy is concerned that small businesses may not understand how their characteristics relate to different parts of the guidance. For example, how do vulnerabilities and risks differ for small and large businesses? What role do small businesses play in broader cyber supply chain risk management? How do in-house cybersecurity measures affect the risk of downstream businesses? How feasible are each of NIST's recommendations for small businesses? Which

---

[2] National Institute of Standards and Technology, Cyber Supply Chain Risk Management Practices for Federal Information Systems and Organizations (NIST Special Publication 800-161, April 2015), https://csrc.nist.gov/publications/detail/sp/800-161/final

[3] E.O. 14028, 86 FR 26633, May 12, 2021.

[4] Census Bureau, Statistics of US Businesses: 2018 Annual Data Tables by Establishment Industry (Washington, DC, May 2021), https://www.census.gov/data/tables/2018/econ/susb/2018-susb-annual.html.

[5] Cybersecurity Maturity Model Certification, Version 1.02 (March, 2020), https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf

recommendations should a business with limited resources focus on? Answering these questions would help small businesses understand why the recommendations matter to them and what they can contribute to cyber supply chain risk management.

3. *NIST should provide a straightforward summary of the most important information.*

Advocacy appreciates NIST's efforts to make this publication more modular and consumable. For small businesses, however, the publication is still long and complex. NIST already presents easy-to-read summaries in its Small Business Cybersecurity Corner. Providing a similar summary for this publication or a reference to the relevant page on the Cybersecurity Corner website would help many small businesses understand the material.

4. *NIST should discuss how components of this guidance relate to recent cybersecurity policies.*

Other policies, including E.O. 14028 and DOD's Cybersecurity Maturity Model Certification (CMMC) framework, will relate to NIST's guidance in important ways for many industries. By discussing these relationships, NIST could help answer many questions that small businesses may have about the landscape of requirements and guidance. For example, where do NIST recommendations overlap or elaborate on components of the executive order requirements, or where might they conflict? Similarly, do any parts of the NIST guidance line up with one of DOD's CMMC levels?

5. *NIST should consider some of the bigger cybersecurity issues that small businesses face.*

Advocacy is also concerned about broader cybersecurity issues for small businesses. As the complexity and types of cybersecurity measures increase, computer security companies often market packages of security software as cure-alls. Small businesses, unable to decipher which elements matter for their particular businesses, may end up paying for much more than they need. Small businesses that work with multiple large clients may also have to comply with different sets of cybersecurity requirements for each contractor, further raising costs. As the push for cyber insurance grows, small businesses frequently purchase the highest-cost policy assuming it provides blanket coverage, only to find out that number or type limitations leave the business vulnerable to large financial burdens.

Advocacy's primary concern is that small businesses, by virtue of being left out of the discussion in this guidance, may be left out of consideration as NIST develops best practices and will be unable to understand how or why this information is important to them. Advocacy recommends that NIST alleviate these issues by considering and discussing how the recommendations might become de facto requirements, the number and characteristics of affected small businesses, how parts of this guidance pertain to them, and how the recommendations relate to broader small business cybersecurity issues, as well as by providing summary information that small businesses can easily consume.

Recommendations

Advocacy applauds NIST's efforts to update its risk management guidance to match new innovations and to present this information in a more consumable way.

Advocacy recommends that NIST discuss the potential for components of this guidance to become de facto requirements and the ramifications for small businesses if that happens. Advocacy also recommends that NIST discuss affected small businesses in more depth and give their risks and needs greater consideration. Describing the number and type of small businesses in the cyber supply chain, how their risks differ from those of large businesses, and which components of the guidance are feasible and most important for reducing risk would help small businesses understand how the content relates to their operations.

Advocacy asks that NIST prepare a summary of this publication's recommendations that small businesses can easily understand and either include or reference that summary near the beginning of this publication.

Advocacy also believes that small businesses would benefit from a discussion of the relationship between components of this guidance and similar policies such as the executive order on "Improving the Nation's Cybersecurity" and DoD's CMMC framework. Advocacy looks forward to working with NIST to explore these new opportunities and challenges in the cyber supply chain.

If you have any questions, or require additional information, please contact me at 202-205-7150 or major.clark@sba.gov.

Sincerely,

/s/

Major L. Clark, III
Acting Chief Counsel
Office of Advocacy
U.S. Small Business Administration

Cc: Sharon Block, Acting Administrator
Office of Information and Regulatory Affairs
Office of Management and Budget