June 17, 2021

Allan Friedman, PhD
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

Re: Docket No. 210527–0117 – Software Bill of Materials Elements and Considerations

Dear Dr. Friedman:

Thank you for the opportunity to comment on the efforts of the National Telecommunications and Information Administration (NTIA) to publish the minimum elements for a Software Bill of Materials (SBoM). As a Member of Congress with an abiding interest in cybersecurity, including the cybersecurity of Federal networks, I believe NTIA's work on SBoM is critical to improving the transparency and security of the software supply chain for developers, Federal procurement officers, and software operators. I write to strongly encourage NTIA to use the findings of its multi-stakeholder process around software component transparency[1] to publish the minimum elements of a SBoM as quickly as possible.

Executive Order (EO) 14028, "Improving the Nation's Cybersecurity,"[2] contains many important elements, including the implementation of legislation based on recommendations from the Cyberspace Solarium Commission, on which I served. Section 4 of the EO, *Enhancing Software Supply Chain Security,* is focused on improving the security of the software Federal departments and agencies use to perform essential government functions. Fundamental to improving the security of critical software is ensuring that procurement contracts reflect security requirements, and the EO enumerates many of these in subsection (e). Of these requirements, SBoM is perhaps the most important.[3]

As a policymaker, SBoM is attractive for several reasons. Using SBoMs scales well because both generating and auditing them is easily *automatable*. SBoM also provides a *foundational* framework that additional controls can be built on top of, depending on an organization's risk appetite. And SBoM can support a *diversity* of stakeholders, with use cases for software makers, buyers, and users. All of these factors make developing a minimum threshold for what constitutes a SBoM particularly urgent.

In determining the SBoM baseline, exploring use cases is particularly important. Software developers can use SBoM to understand the existence of known vulnerabilities in libraries their code relies on. Developers can also use the data surfaced by creating a SBoM to understand supply chain risks, such as reliance on an open-source component that is being minimally maintained. While it's true that decisions

[1] https://www.ntia.doc.gov/SoftwareTransparency

[2] https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[3] Another important requirement is participation in a vulnerability disclosure program. The findings of NTIA's multi-stakeholder process around cybersecurity vulnerabilities should provide several guideposts for the National Institute of Standards and Technology as it generates its guidance pursuant to subsection (e).

about these types of risk are already regularly made by software engineers, the transparency provided by an SBoM allows other stakeholders, including business risk divisions and security teams, to better understand their exposure. Much of the utility of SBoM for developers derives from the *depth* of dependencies: the shallower the SBoM, the more likely the code in question is written by the software creators themselves. As such, I urge NTIA to set the minimum required depth to be as complete as possible and to maintain requirements for surfacing unknown or partial dependencies.

For software purchasers, auditing is key. While it is true that Federal software acquisition officials should continue to deepen their knowledge of secure software, evaluating the security of code based on a SBoM is unlikely to be one of their core competencies.[4] However, they should be able to quickly determine the existence of a SBoM and its completeness to evaluate whether a piece of software can be purchased by Federal customers. NTIA should therefore continue to emphasize *interoperability*, in conjunction with the EO's requirement for machine readability, as this will enhance the ability of procurement officers to use a common toolset in evaluating SBoM.

A minimum standard for SBoM must also include requirements on *maintenance*; after all, software is updated at a dizzying speed. Federal software licensing contracts must include requirements that updated SBoM be provided in conjunction with feature and security patches. In a similar vein, I hope NTIA will place an emphasis on making SBoM available online whenever possible. In addition to making auditing more automatable, posting SBoMs online also has the potential to help the broader ecosystem of software users, not just Federal government customers. As noted in the EO: "The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, *the private sector* [emphasis added], and ultimately the American people's security and privacy." NTIA must consider the potential benefits to non-Federal users of SBoMs as it deliberates what minimum elements to include.

Software users, and the security teams that protect them, have different use cases for SBoM. When a new vulnerability is discovered in a commonly used software library, the existence of a SBoM can allow cybersecurity operators to quickly assess their exposure. Agency heads can also use SBoM to ensure compliance with security directives issued by the Cybersecurity and Infrastructure Security Agency or new mandates imposed by Congress. Because vulnerability management is a frequently cited use case for SBoM, I encourage NTIA to continue to explore how presenting the particular functions that are actually used in software may increase accuracy of risk assessments. I also urge NTIA to work with the Office of Management and Budget to advocate the use of SBoM for embedded devices that, while not conventionally "software," may nonetheless be supporting critical functions and be vulnerable to cyber intrusions.

Finally, I encourage NTIA to avoid projecting how its standards may affect Federal contracting. The cost to generate and maintain an SBoM is an important consideration in determining which minimum elements to include. However, NTIA should not attempt to guess how SBoM requirements might affect future contract negotiations carried out by the General Services Administration and other departments and agencies. The Federal Government's purchasing power is immense, and NTIA should not limit the ability of procurement officers to strike the best possible deal for Federal customers. Increased software transparency may, indeed, impose costs on software developers wishing to sell to the Federal Government by forcing them to alter terms of existing license arrangements. However, I firmly believe that our unwillingness to pay for security is one of the reasons we continue to face the volume of cyber threats that we do. What's more, the best time to determine the actual cost of revealing any "sensitive" information

[4] I hope that the Office of Management and Budget will consider including testing and evaluation of software by trained experts in its procurement guidance; however, I do not believe that such testing and evaluation can effectively be carried out by acquisition officials. Regardless of whether such testing – which may benefit from the availability of SBoMs – is carried out, SBoMs will provide significant benefits for Federal cybersecurity.

that might be included in a SBoM is during the bidding process and contract negotiations, not during the development of the SBoM minimal elements.

Thank you again for the opportunity to comment on this important issue. I again commend NTIA for its work with stakeholders in exploring SBoM policy over the past three years. Without the groundwork laid through years of research, engagement, and problem solving, we would not be at the crux of implementing this momentous change in software security.

I look forward to continuing to work with NTIA and other elements of the administration to implement the EO and improve Federal cybersecurity. If you have any questions regarding this submittal, please contact my office at (202) 225-2735.

Sincerely,

JAMES R. LANGEVIN
Member of Congress

cc: Dr. Charles H. Romine, Director, Information Technology Laboratory, NIST

JAMES R. LANGEVIN
2nd District, Rhode Island

COMMITTEE ON ARMED SERVICES
Intelligence and Emerging Threats
and Capabilities (Chairman)
Seapower and Projection Forces
Tactical Air and Land Forces

COMMITTEE ON
HOMELAND SECURITY
Cybersecurity, Infrastructure
Protection, and Innovation
Intelligence and Counterterrorism

Congress of the United States
House of Representatives
Washington, DC 20515–3902

Washington Office:
2077 Rayburn House Office Building
Washington, DC 20515
Telephone: (202) 225–2735
Fax: (202) 225–5976

District Office:
The Summit South
300 Centerville Road, Suite 200
Warwick, RI 02886
Telephone: (401) 732–9400
Fax: (401) 737–2982

https://langevin.house.gov

June 17, 2021

Allan Friedman, PhD
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

Re: Docket No. 210527–0117 – Software Bill of Materials Elements and Considerations

Dear Dr. Friedman:

Thank you for the opportunity to comment on the efforts of the National Telecommunications and Information Administration (NTIA) to publish the minimum elements for a Software Bill of Materials (SBoM). As a Member of Congress with an abiding interest in cybersecurity, including the cybersecurity of Federal networks, I believe NTIA's work on SBoM is critical to improving the transparency and security of the software supply chain for developers, Federal procurement officers, and software operators. I write to strongly encourage NTIA to use the findings of its multi-stakeholder process around software component transparency[1] to publish the minimum elements of a SBoM as quickly as possible.

Executive Order (EO) 14028, "Improving the Nation's Cybersecurity,"[2] contains many important elements, including the implementation of legislation based on recommendations from the Cyberspace Solarium Commission, on which I served. Section 4 of the EO, *Enhancing Software Supply Chain Security*, is focused on improving the security of the software Federal departments and agencies use to perform essential government functions. Fundamental to improving the security of critical software is ensuring that procurement contracts reflect security requirements, and the EO enumerates many of these in subsection (e). Of these requirements, SBoM is perhaps the most important.[3]

As a policymaker, SBoM is attractive for several reasons. Using SBoMs scales well because both generating and auditing them is easily *automatable*. SBoM also provides a *foundational* framework that additional controls can be built on top of, depending on an organization's risk appetite. And SBoM can support a *diversity* of stakeholders, with use cases for software makers, buyers, and users. All of these factors make developing a minimum threshold for what constitutes a SBoM particularly urgent.

In determining the SBoM baseline, exploring use cases is particularly important. Software developers can use SBoM to understand the existence of known vulnerabilities in libraries their code relies on. Developers can also use the data surfaced by creating a SBoM to understand supply chain risks, such as reliance on an open-source component that is being minimally maintained. While it's true that decisions

[1] https://www.ntia.doc.gov/SoftwareTransparency

[2] https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[3] Another important requirement is participation in a vulnerability disclosure program. The findings of NTIA's multi-stakeholder process around cybersecurity vulnerabilities should provide several guideposts for the National Institute of Standards and Technology as it generates its guidance pursuant to subsection (e).

about these types of risk are already regularly made by software engineers, the transparency provided by an SBoM allows other stakeholders, including business risk divisions and security teams, to better understand their exposure. Much of the utility of SBoM for developers derives from the *depth* of dependencies: the shallower the SBoM, the more likely the code in question is written by the software creators themselves. As such, I urge NTIA to set the minimum required depth to be as complete as possible and to maintain requirements for surfacing unknown or partial dependencies.

For software purchasers, auditing is key. While it is true that Federal software acquisition officials should continue to deepen their knowledge of secure software, evaluating the security of code based on a SBoM is unlikely to be one of their core competencies.[4] However, they should be able to quickly determine the existence of a SBoM and its completeness to evaluate whether a piece of software can be purchased by Federal customers. NTIA should therefore continue to emphasize *interoperability*, in conjunction with the EO's requirement for machine readability, as this will enhance the ability of procurement officers to use a common toolset in evaluating SBoM.

A minimum standard for SBoM must also include requirements on *maintenance*; after all, software is updated at a dizzying speed. Federal software licensing contracts must include requirements that updated SBoM be provided in conjunction with feature and security patches. In a similar vein, I hope NTIA will place an emphasis on making SBoM available online whenever possible. In addition to making auditing more automatable, posting SBoMs online also has the potential to help the broader ecosystem of software users, not just Federal government customers. As noted in the EO: "The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, *the private sector* [emphasis added], and ultimately the American people's security and privacy." NTIA must consider the potential benefits to non-Federal users of SBoMs as it deliberates what minimum elements to include.

Software users, and the security teams that protect them, have different use cases for SBoM. When a new vulnerability is discovered in a commonly used software library, the existence of a SBoM can allow cybersecurity operators to quickly assess their exposure. Agency heads can also use SBoM to ensure compliance with security directives issued by the Cybersecurity and Infrastructure Security Agency or new mandates imposed by Congress. Because vulnerability management is a frequently cited use case for SBoM, I encourage NTIA to continue to explore how presenting the particular functions that are actually used in software may increase accuracy of risk assessments. I also urge NTIA to work with the Office of Management and Budget to advocate the use of SBoM for embedded devices that, while not conventionally "software," may nonetheless be supporting critical functions and be vulnerable to cyber intrusions.

Finally, I encourage NTIA to avoid projecting how its standards may affect Federal contracting. The cost to generate and maintain an SBoM is an important consideration in determining which minimum elements to include. However, NTIA should not attempt to guess how SBoM requirements might affect future contract negotiations carried out by the General Services Administration and other departments and agencies. The Federal Government's purchasing power is immense, and NTIA should not limit the ability of procurement officers to strike the best possible deal for Federal customers. Increased software transparency may, indeed, impose costs on software developers wishing to sell to the Federal Government by forcing them to alter terms of existing license arrangements. However, I firmly believe that our unwillingness to pay for security is one of the reasons we continue to face the volume of cyber threats that we do. What's more, the best time to determine the actual cost of revealing any "sensitive" information

[4] I hope that the Office of Management and Budget will consider including testing and evaluation of software by trained experts in its procurement guidance; however, I do not believe that such testing and evaluation can effectively be carried out by acquisition officials. Regardless of whether such testing – which may benefit from the availability of SBoMs – is carried out, SBoMs will provide significant benefits for Federal cybersecurity.

that might be included in a SBoM is during the bidding process and contract negotiations, not during the development of the SBoM minimal elements.

Thank you again for the opportunity to comment on this important issue. I again commend NTIA for its work with stakeholders in exploring SBoM policy over the past three years. Without the groundwork laid through years of research, engagement, and problem solving, we would not be at the crux of implementing this momentous change in software security.

I look forward to continuing to work with NTIA and other elements of the administration to implement the EO and improve Federal cybersecurity. If you have any questions regarding this submittal, please contact my office at (202) 225-2735.

Sincerely,

Jim Langevin

JAMES R. LANGEVIN
Member of Congress

cc: Dr. Charles H. Romine, Director, Information Technology Laboratory, NIST