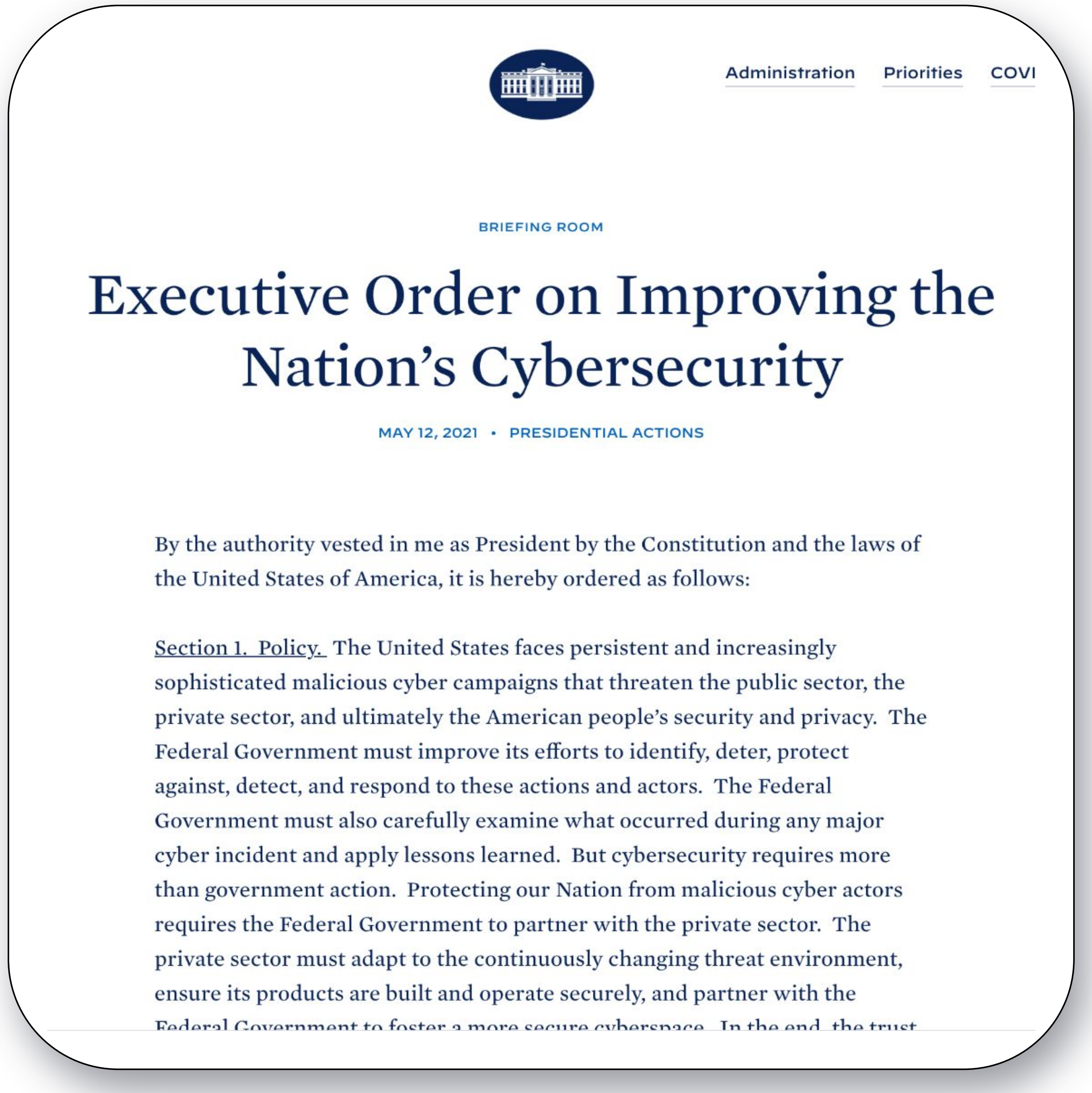
TIDELIFT BRIEFING

Thinking upstream about White House cybersecurity executive order 14028

TIDELIFT

What you need to know



BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

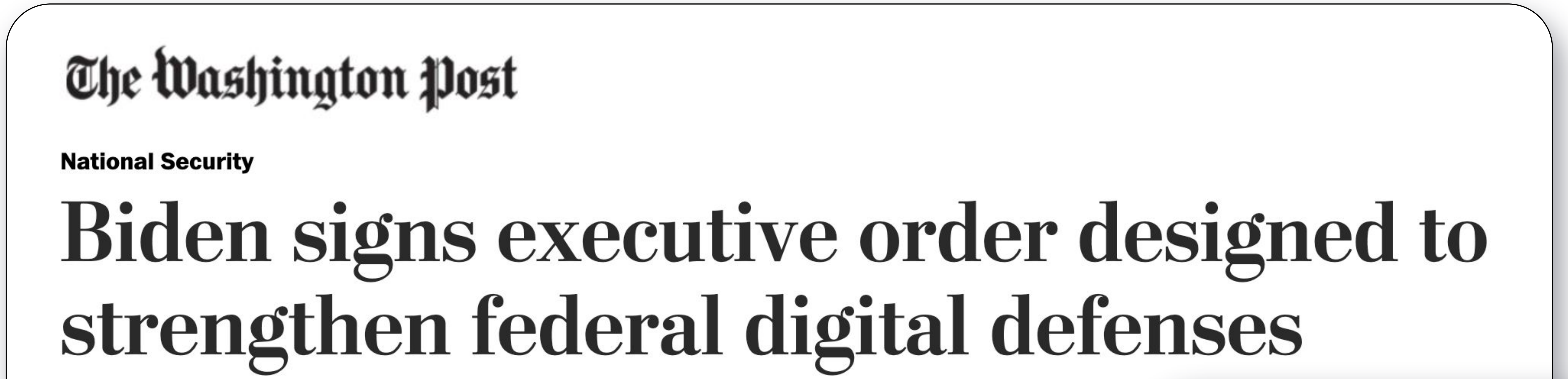
MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust

1. In May, the White House released an executive order with detailed directives on improving the nation's cybersecurity
2. This is the government's response to the recent set of high-profile attacks like the one affecting SolarWinds customers
3. Potentially large impacts on organizations using open source to develop applications, more details and standards emerging every day

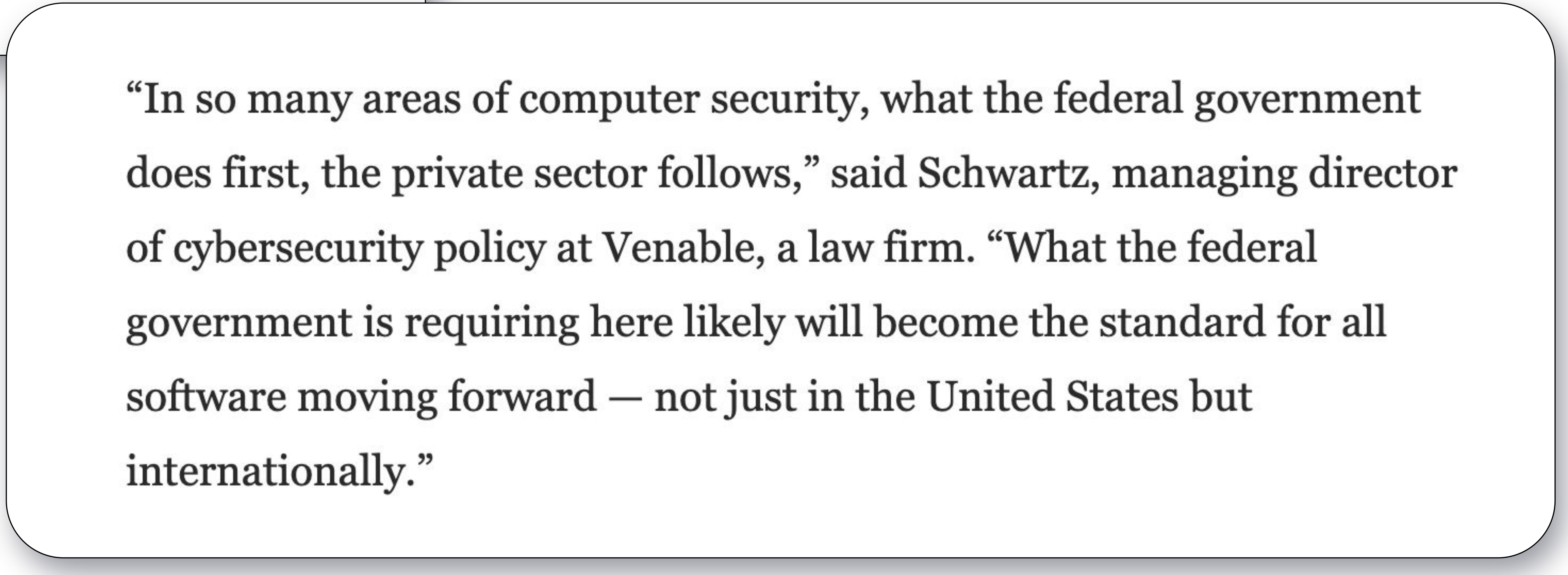
Why this should matter to every organization



The Washington Post

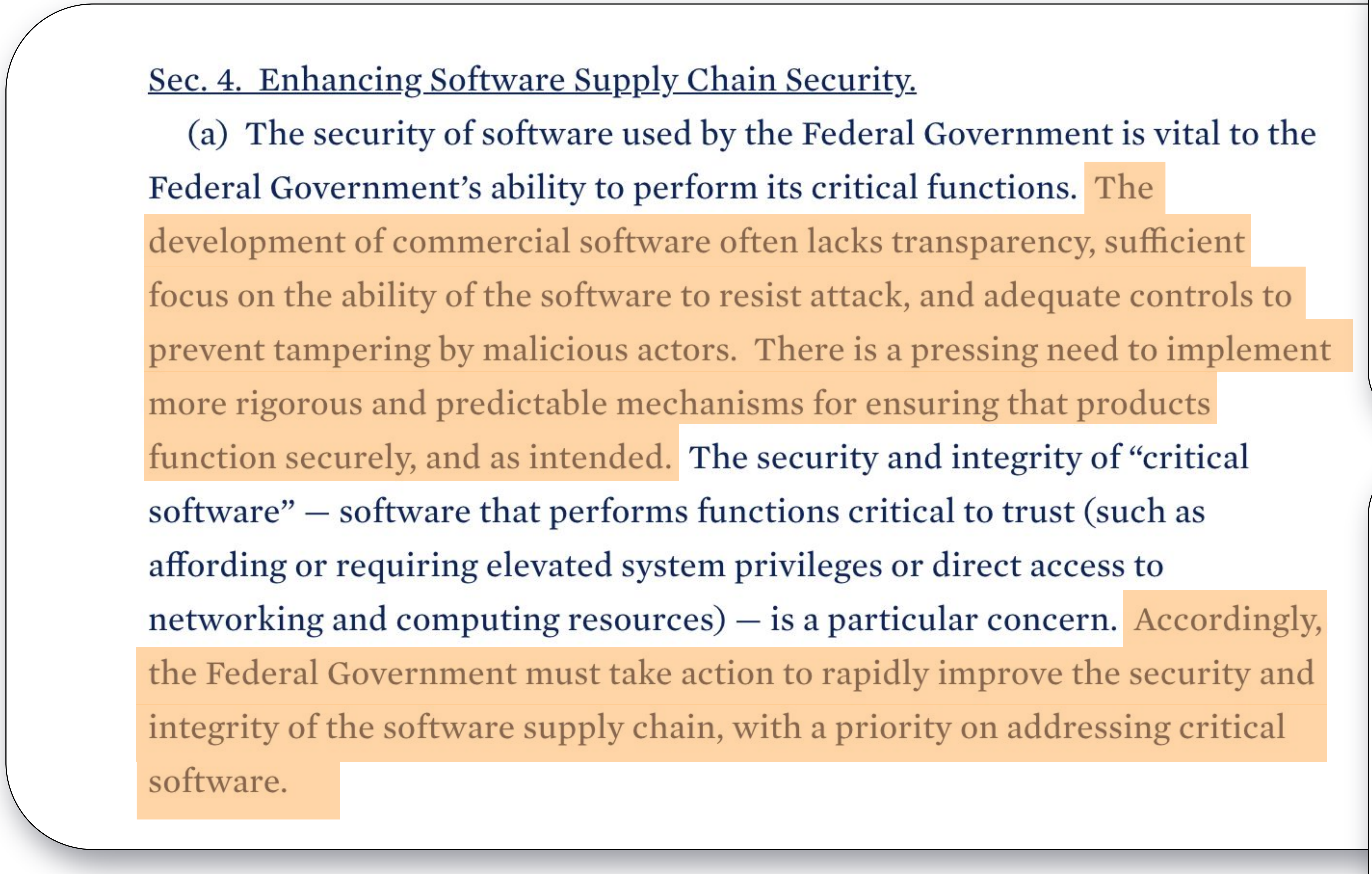
National Security

Biden signs executive order designed to strengthen federal digital defenses



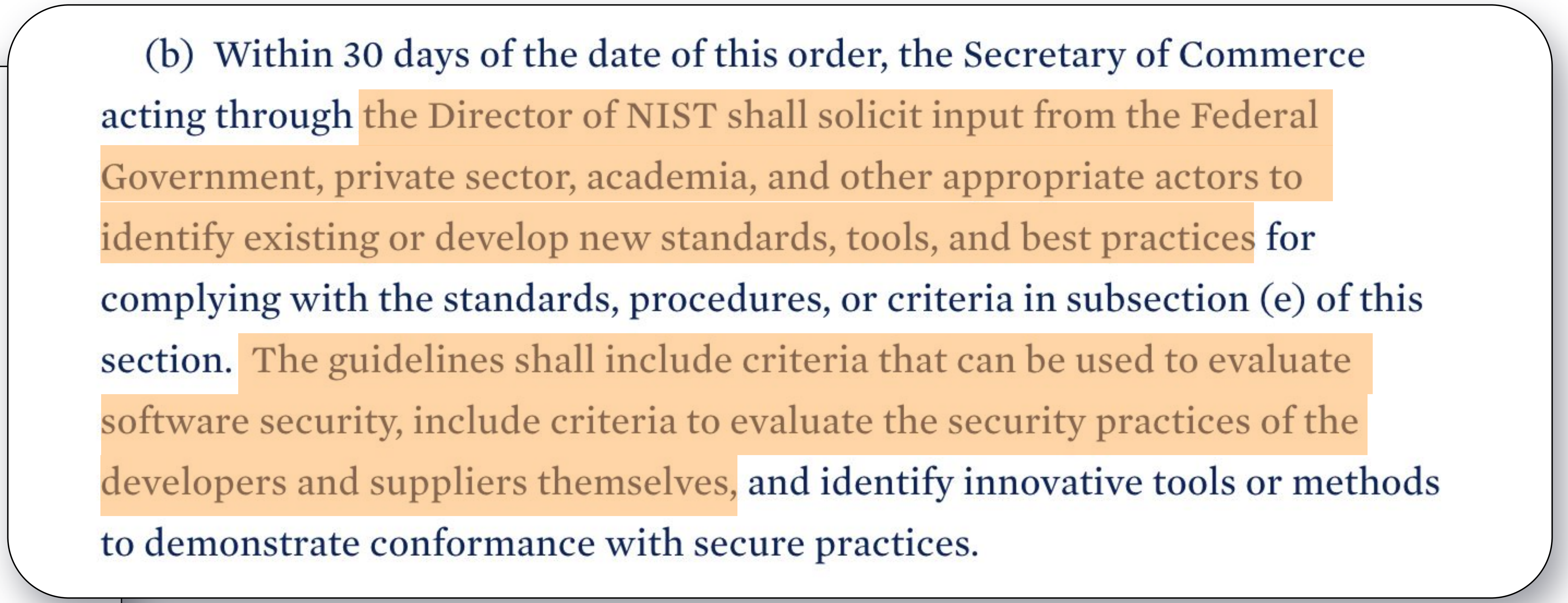
“In so many areas of computer security, what the federal government does first, the private sector follows,” said Schwartz, managing director of cybersecurity policy at Venable, a law firm. “What the federal government is requiring here likely will become the standard for all software moving forward — not just in the United States but internationally.”

One critical area of focus for app dev teams: software supply chain security

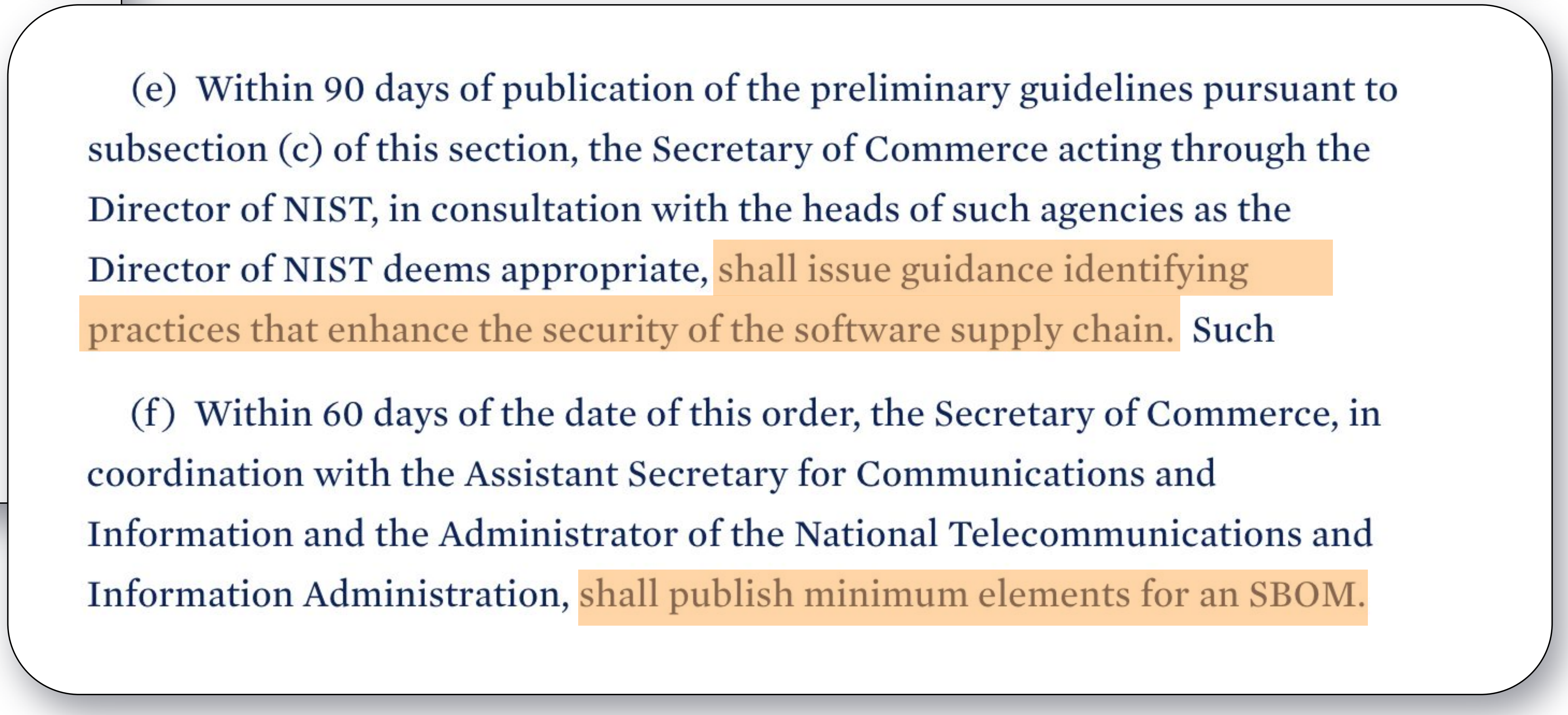


Sec. 4. Enhancing Software Supply Chain Security.

(a) The security of software used by the Federal Government is vital to the Federal Government's ability to perform its critical functions. The development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors. There is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended. The security and integrity of "critical software" — software that performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources) — is a particular concern. Accordingly, the Federal Government must take action to rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software.



(b) Within 30 days of the date of this order, the Secretary of Commerce acting through the Director of NIST shall solicit input from the Federal Government, private sector, academia, and other appropriate actors to identify existing or develop new standards, tools, and best practices for complying with the standards, procedures, or criteria in subsection (e) of this section. The guidelines shall include criteria that can be used to evaluate software security, include criteria to evaluate the security practices of the developers and suppliers themselves, and identify innovative tools or methods to demonstrate conformance with secure practices.



(e) Within 90 days of publication of the preliminary guidelines pursuant to subsection (c) of this section, the Secretary of Commerce acting through the Director of NIST, in consultation with the heads of such agencies as the Director of NIST deems appropriate, shall issue guidance identifying practices that enhance the security of the software supply chain. Such

(f) Within 60 days of the date of this order, the Secretary of Commerce, in coordination with the Assistant Secretary for Communications and Information and the Administrator of the National Telecommunications and Information Administration, shall publish minimum elements for an SBOM.

NIST
Search NIST
Menu

Information Technology Laboratory

EXECUTIVE ORDER 14028, IMPROVING THE NATION'S CYBERSECURITY

Critical Software
Critical Software Definition
Security Measures for Critical Software Use
Introduction
Purpose & Scope
Security Measures for EO-Critical Software Use
FAQs
Software Verification
Cybersecurity Labeling for Consumers
Workshops & Call for Papers
News & Updates
Engage
Fact Sheet
Resources
FAQs

Security Measures for EO-Critical Software Use

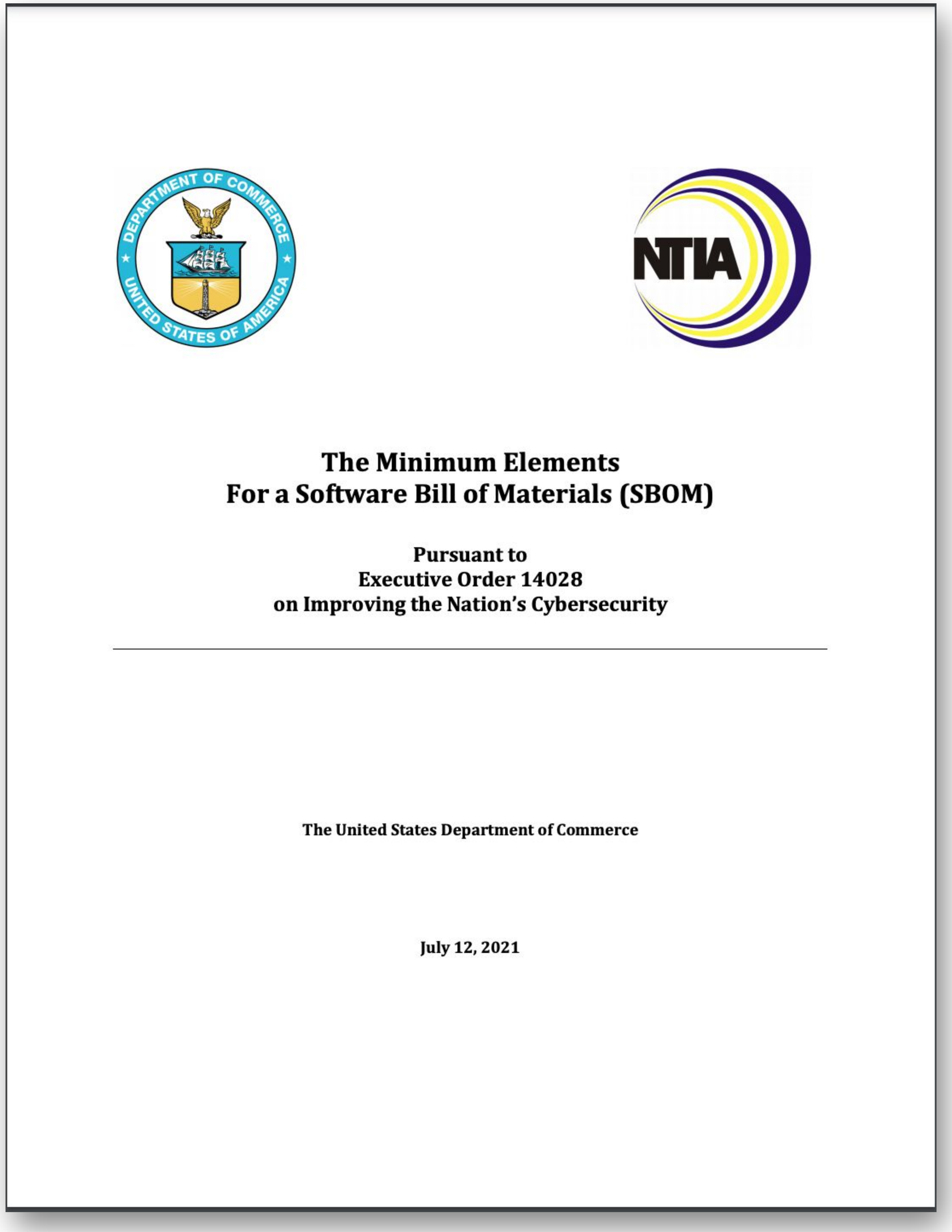
The table below defines the security measures for EO-critical software use. The security measures are grouped by objective. The columns in the table are:

- **Security Measure (SM)**: A high-level security outcome statement that is intended to apply to all software designated as EO-critical so
software
- **Federal**
discuss
NIST Sp
These tw
security
differen

All referenc
sources of in
does not imply that other sources of information should not be used.

The references listed in the table will be updated periodically as new publications are identified or released, and as existing publications are updated.

Objective 3: Identify and maintain EO-critical software platforms and the software deployed to those platforms to protect the EO-critical software from exploitation.	
SM 3.1: Establish and maintain a software inventory for all platforms running EO-critical software and all software (both EO-critical and non-EO-critical) deployed to each platform.	- **NIST,** Cybersecurity Framework: ID.AM-1, ID.AM-2, ID.SC-2 - **NIST,** SP 800-53 Rev. 5, Security and

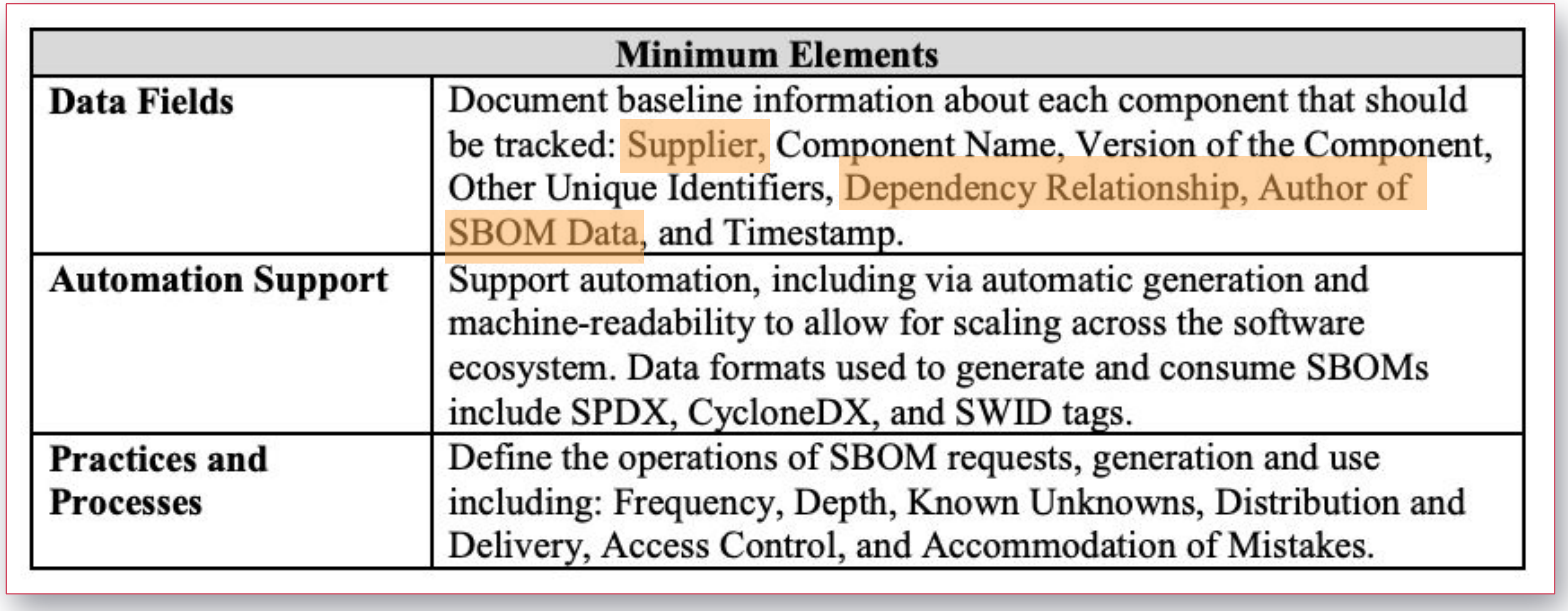


The Minimum Elements
For a Software Bill of Materials (SBOM)

Pursuant to
Executive Order 14028
on Improving the Nation's Cybersecurity

The United States Department of Commerce

July 12, 2021

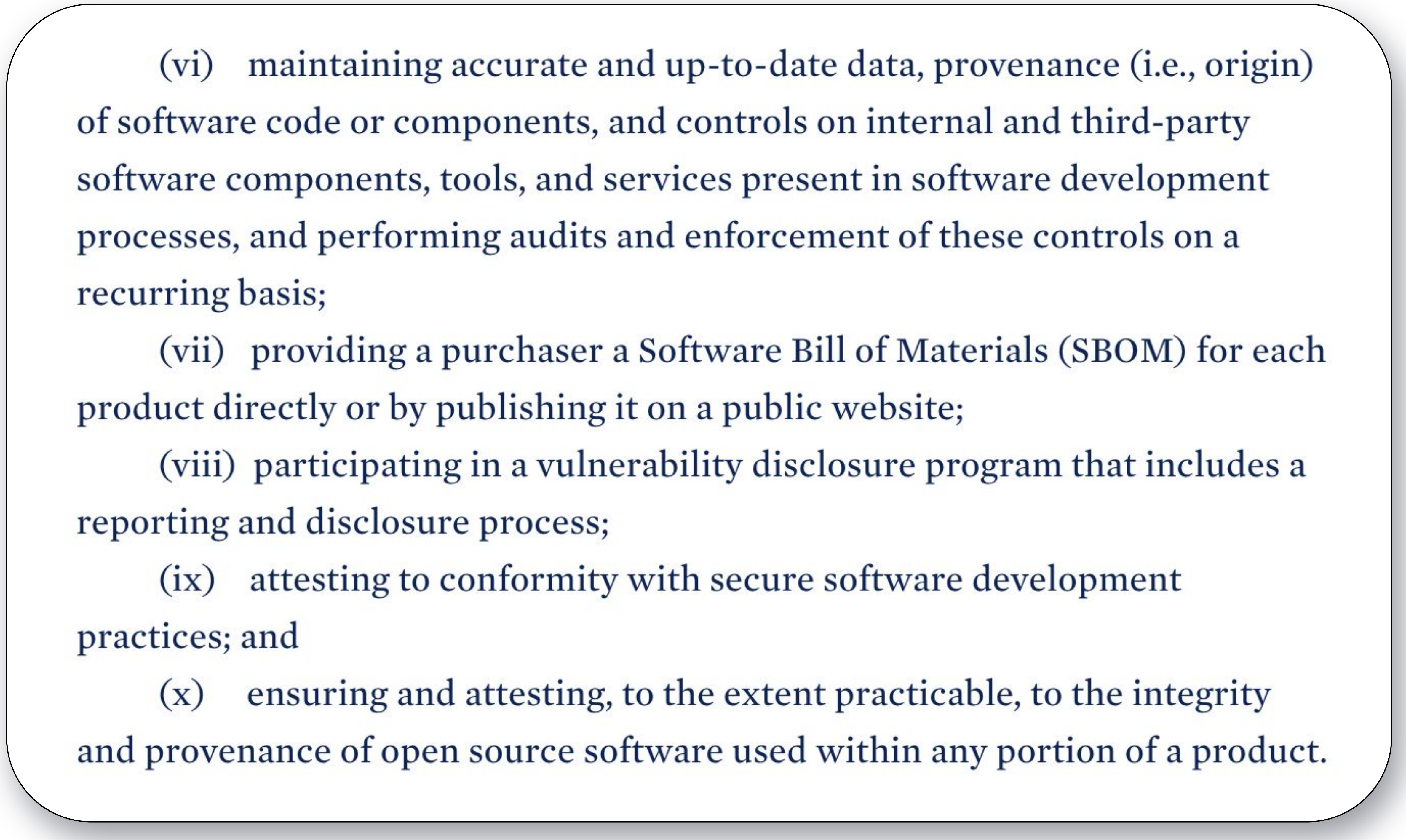


Minimum Elements	
Data Fields	Document baseline information about each component that should be tracked: Supplier, Component Name, Version of the Component, Other Unique Identifiers, Dependency Relationship, Author of SBOM Data, and Timestamp.
Automation Support	Support automation, including via automatic generation and machine-readability to allow for scaling across the software ecosystem. Data formats used to generate and consume SBOMs include SPDX, CycloneDX, and SWID tags.
Practices and Processes	Define the operations of SBOM requests, generation and use including: Frequency, Depth, Known Unknowns, Distribution and Delivery, Access Control, and Accommodation of Mistakes.

Which leads us to some key questions...

If you are building applications
with open source, how do you:

1. track and maintain an accurate software inventory / bill of materials?
2. “attest to the integrity and provenance of open source software”?
3. “attest to conformity with secure software development practices”?



(vi) maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and controls on internal and third-party software components, tools, and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis;

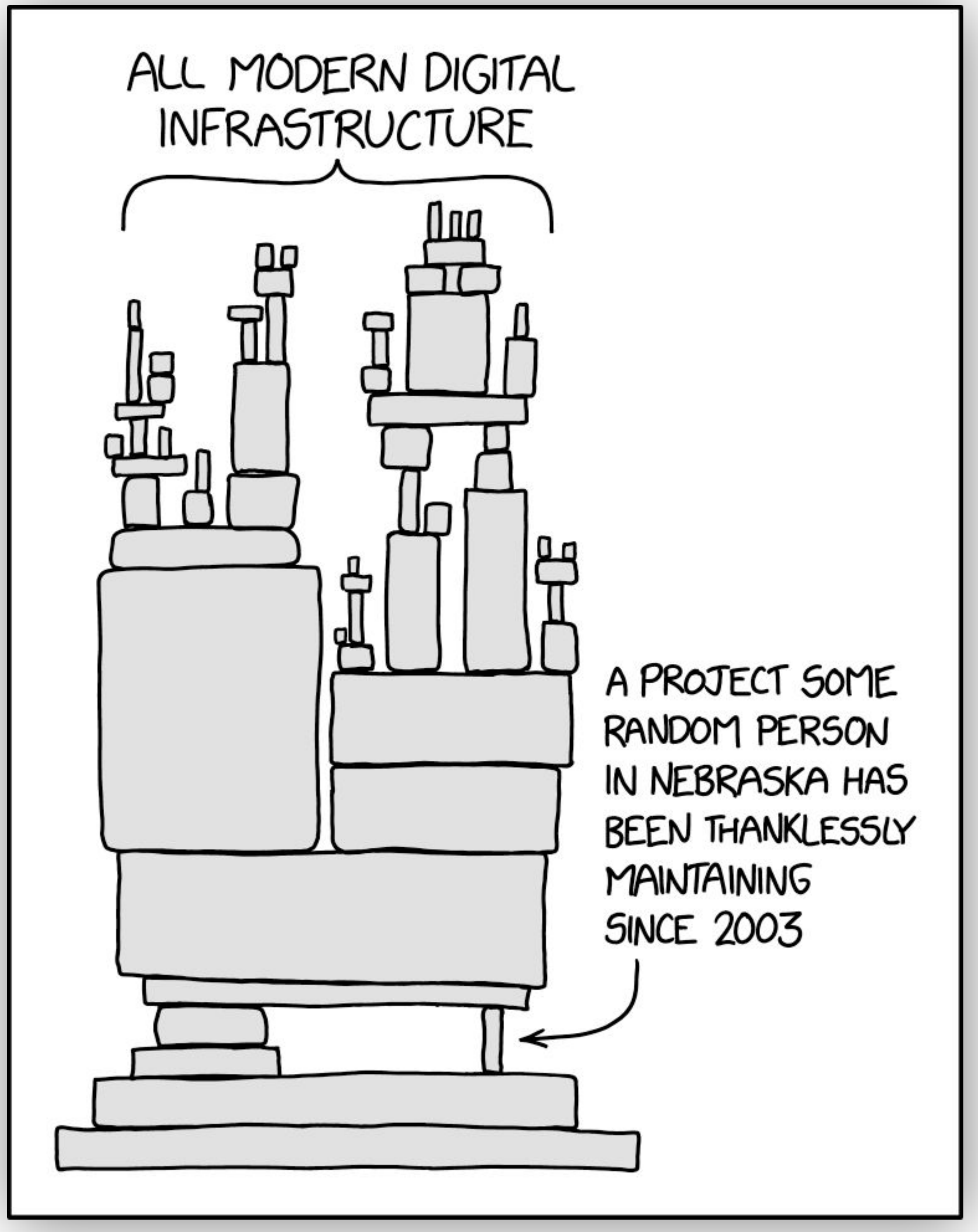
(vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;

(viii) participating in a vulnerability disclosure program that includes a reporting and disclosure process;

(ix) attesting to conformity with secure software development practices; and

(x) ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion of a product.

Especially when the reality looks like this:

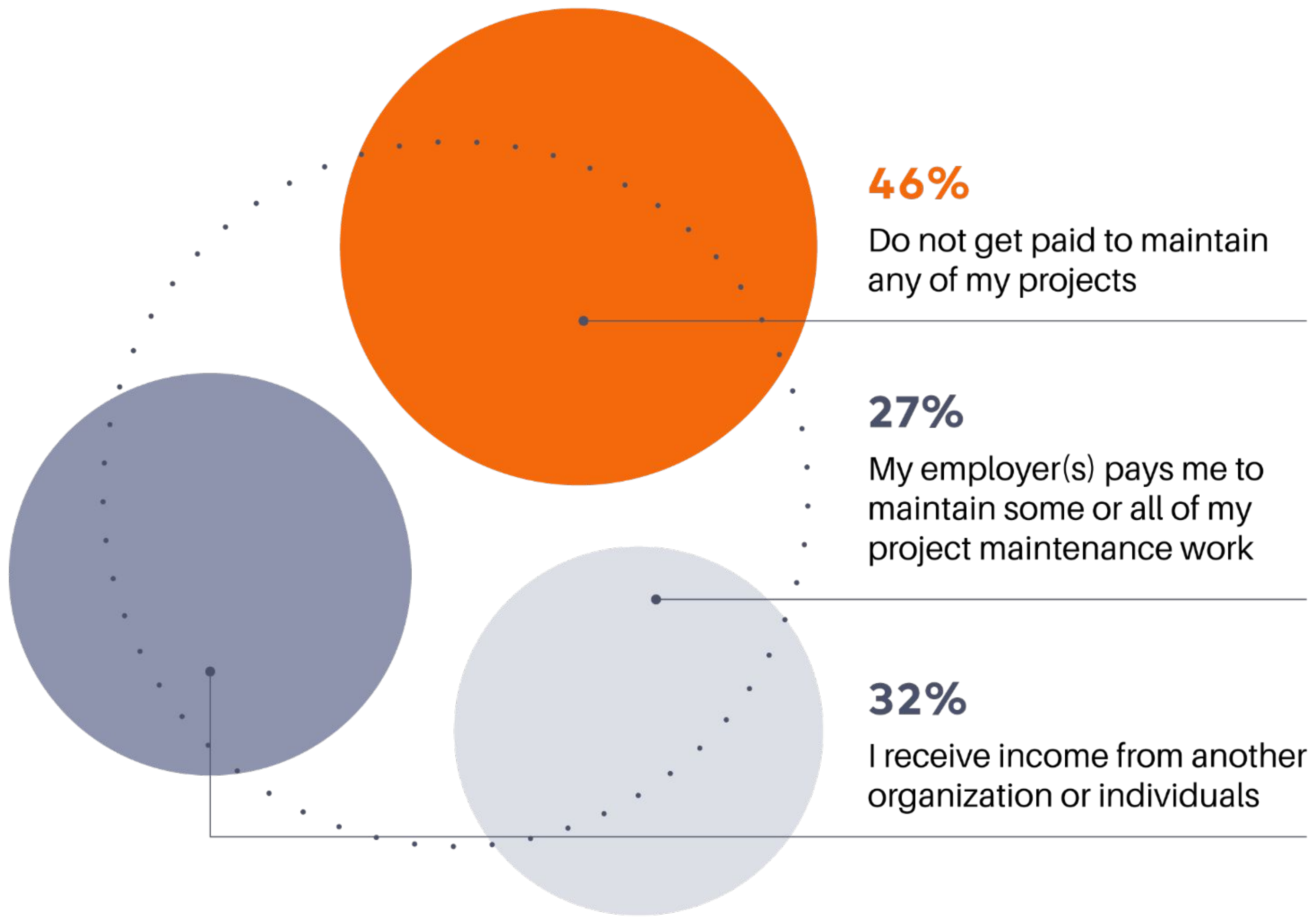

ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

Source: xkcd https://xkcd.com/2347/

And this...

About half of maintainers get paid nothing for their work

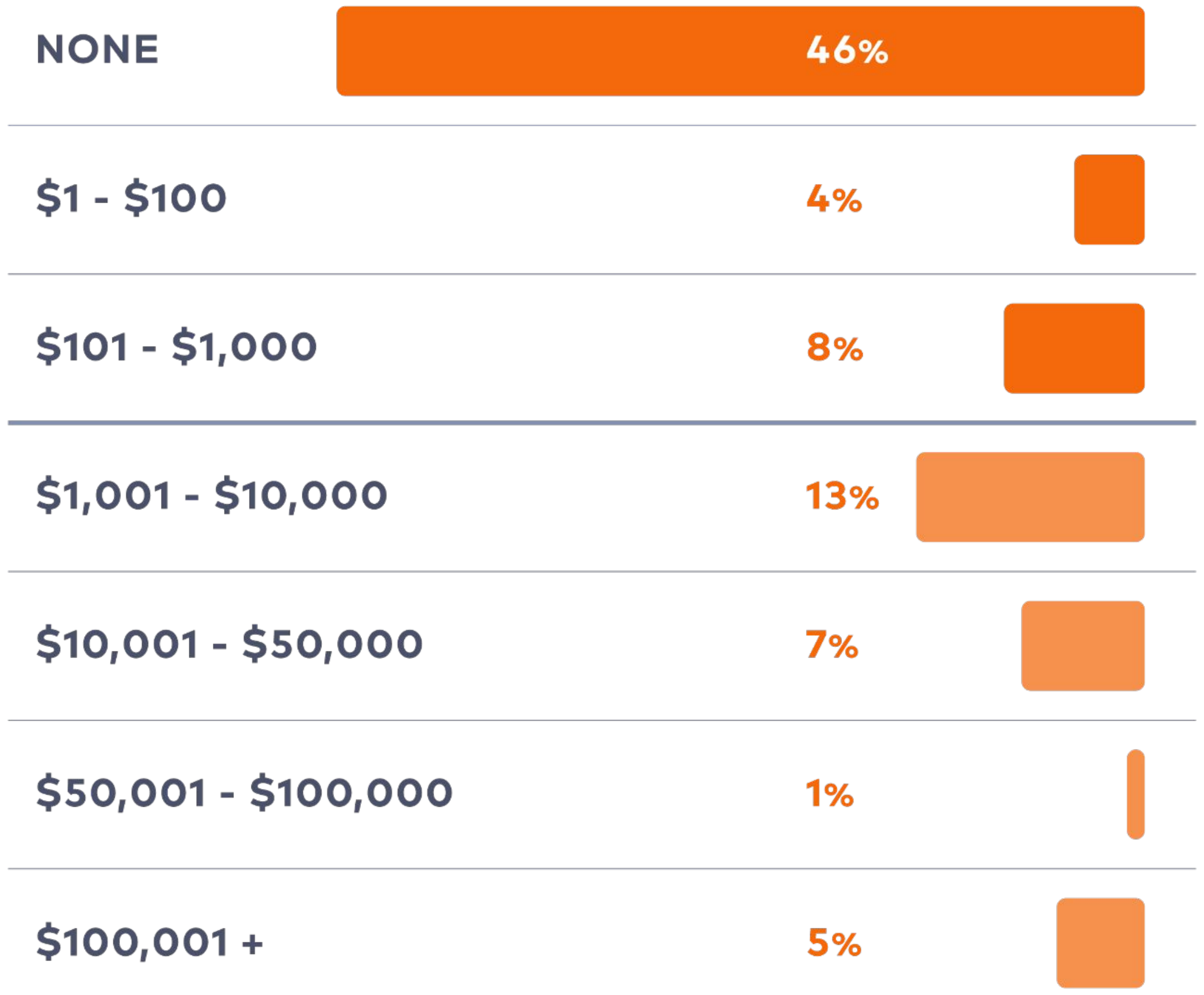
Which of the following describe how you currently fund your open source project maintenance work? (Choose all that apply)



n=378 | More than one option could be selected

Only 1/4 of maintainers earn more than $1K per year for their maintenance work

How much total income do you receive per year for your open source maintenance work from all sources?



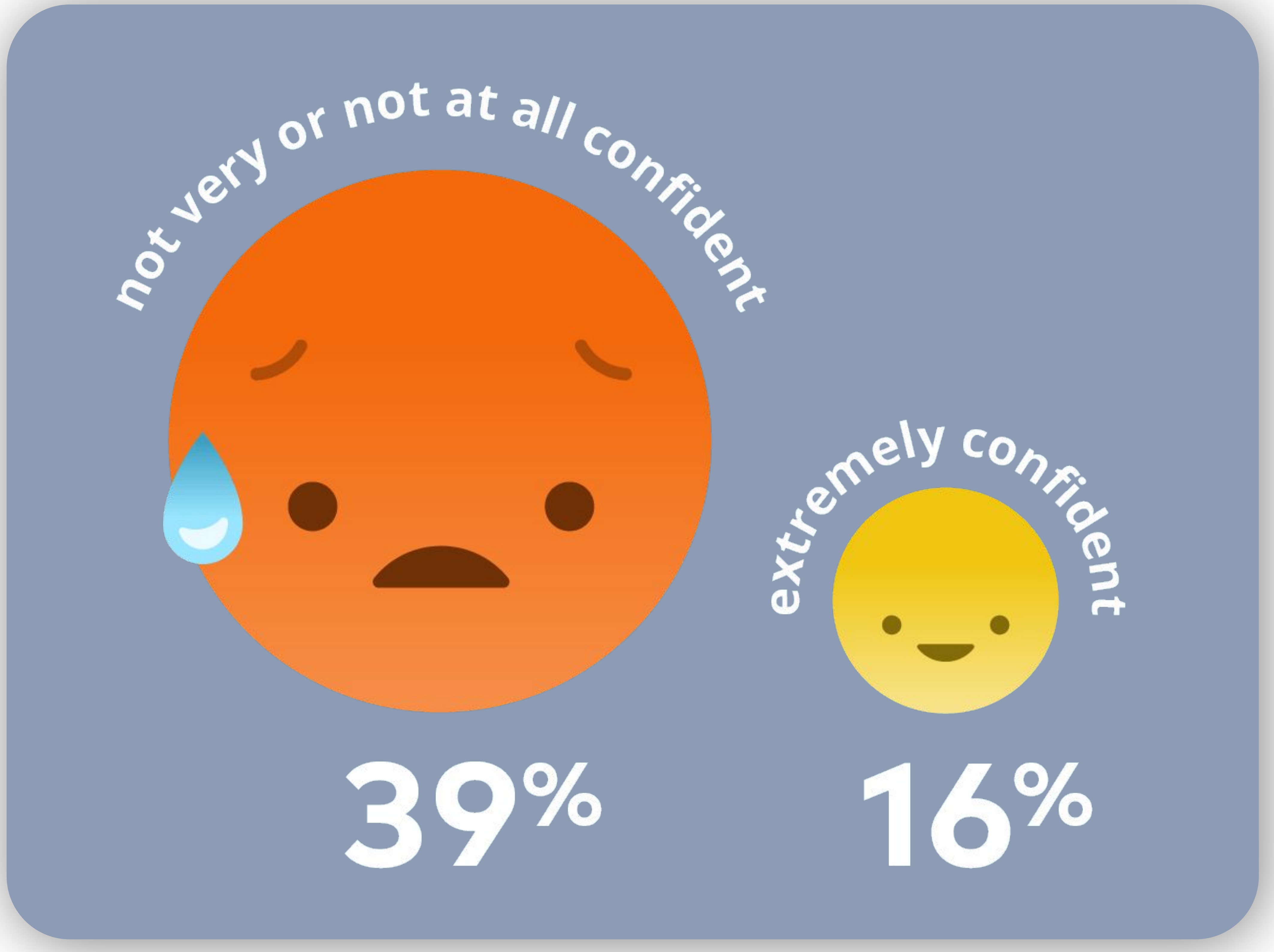
n=361 | "None" includes respondents that previously indicated they do not get paid. Results do not equal 100% because "Don't know" and non-responses are not shown.

Source: 2021 Tidelift Maintainer Survey

And this...

In a recent survey, we asked organizations with more than 10,000 employees:

> **How confident are you that the open source components in use today at your organization are up to date, secure, and well maintained?**



Source: 2020 Tidelift Managed Open Source Survey

The upstream parable

When it comes to addressing the issues raised by the executive order, what would be an upstream solution for application development teams?

Key issues for application development teams using open source

1. How do I produce and maintain an accurate SBOM for my projects?

2. How can I feel confident attesting to the integrity and provenance of open source software components?

3. How can I feel confident attesting to how open source components conform to secure software development practices?

What if we enlisted the help of the people who created the software?

The Tidelift Subscription

A better way for organizations to manage their open source software supply chain.

Reduce the complexity of managing open source components, while keeping them safe and up to date with help from Tidelift and our growing network of partnered maintainers.

Cut costs

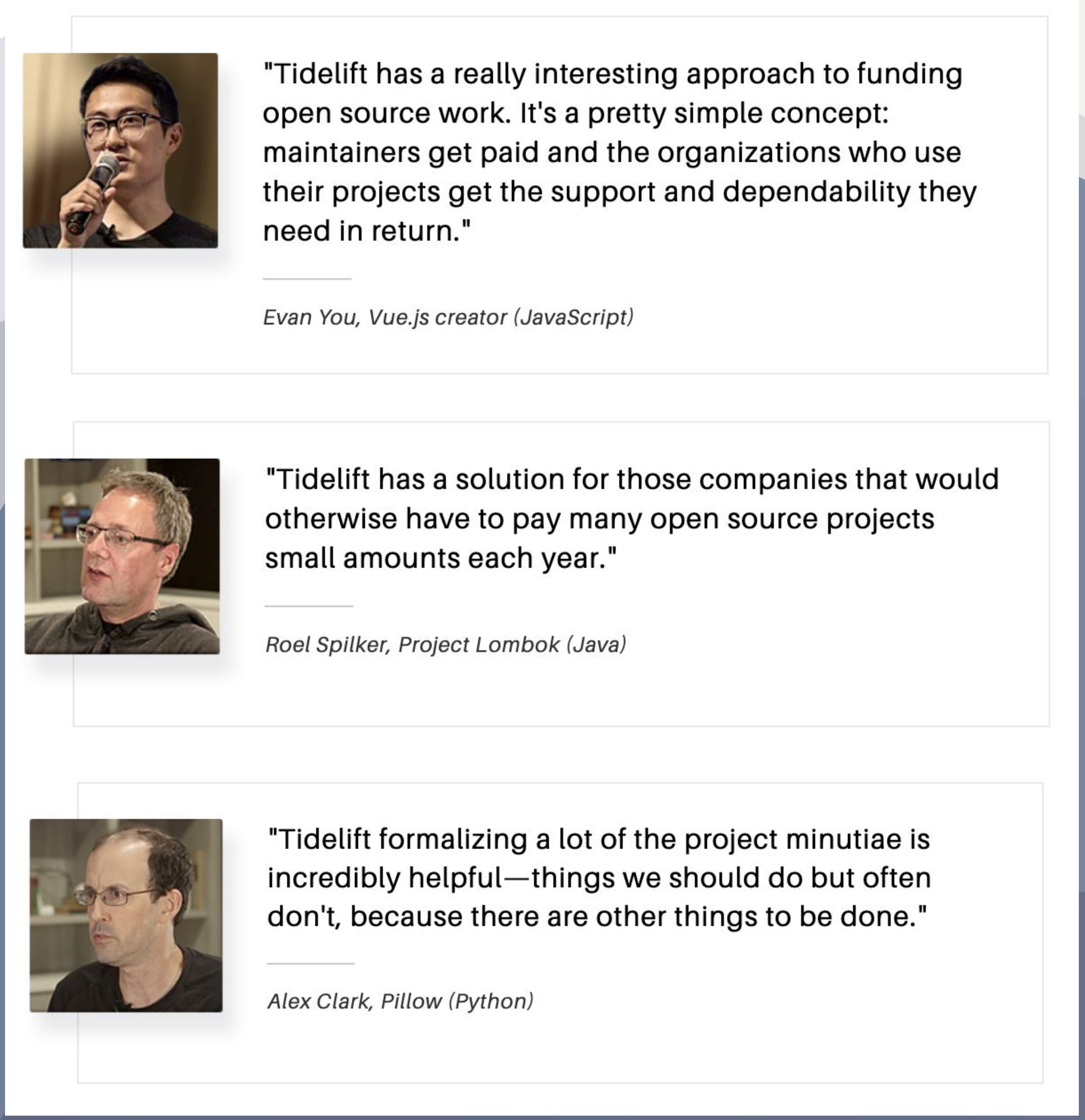
Accelerate development

Reduce risk

Backed by maintainers

Tidelift partners directly with the independent maintainers behind thousands of open source projects—with more added every day.

The more subscribers using a project, the more its maintainers get paid. Which means they can dedicate even more time to maintenance and security tasks, while continuing to invest in making their projects even better.



"Tidelift has a really interesting approach to funding open source work. It's a pretty simple concept: maintainers get paid and the organizations who use their projects get the support and dependability they need in return."

Evan You, Vue.js creator (JavaScript)

"Tidelift has a solution for those companies that would otherwise have to pay many open source projects small amounts each year."

Roel Spilker, Project Lombok (Java)

"Tidelift formalizing a lot of the project minutiae is incredibly helpful—things we should do but often don't, because there are other things to be done."

Alex Clark, Pillow (Python)

What’s included in the Tidelift Subscription

TOOLS

We provide the tools to curate, track, and manage catalogs of open source components and the policies that govern them. We also integrate seamlessly with your existing repository management solutions like GitHub, GitLab, and JFrog Artifactory.

MAINTAINERS

We partner with a large and fast-growing network of open source maintainers who create and maintain the dependencies you use every day, paying them to keep their code secure and up to date—now and into the future.

MANAGEMENT

We provide expert data, recommendations, and resources to help you proactively manage components consistently across the organization, keeping your developers moving fast and staying safe.

Get a free trial of

the Tidelift Subscription

tidelift.com/subscription/free-trial

TIDELIFT