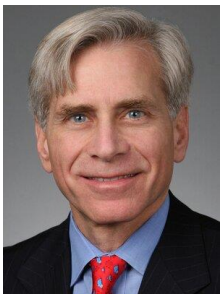
# 3 Cybersecurity Takeaways From White House Tech Report

By **Alan Raul, Stephen McInerney and Vishnu Tirumala** (March 26, 2024)



Alan Raul

Stephen McInerney

Vishnu Tirumala

On Feb. 26, the White House's Office of the National Cyber Director, or ONCD, released a report on how technology manufacturers and software developers can improve the cybersecurity posture of the U.S.[1]

This report, "Back to the Building Blocks: A Path Toward Secure and Measurable Software," is in lockstep with the Biden administration's intense focus on software development and its stated objective to move the needle on software manufacturer accountability.

Taking stock of the administration's push on software security will be important for tech companies and software developers — and their boards of directors and CEOs, who the White House says are "ultimately accountable."[2]

**Background on the Paradigm Shift for Software Development**

Before outlining our key takeaways from the report, it is important to appreciate two facts that provide context for this report:

***1. Rising geopolitical tensions extend into cyberspace.***

Over the last few months, the U.S. government has repeatedly sounded alarm bells about — and fought back against — the increased threat of sophisticated cyberattacks against the U.S. and its critical infrastructure.

On Jan. 31, before the House Select Committee on the Chinese Communist Party, the nation's top cybersecurity officials testified that in the event of a conflict with China, the Chinese government could carry out a "cyber invasion" of our IT infrastructure. "This is truly an everything, everywhere, all at once scenario," Cybersecurity and Infrastructure Security Agency Director Jen Easterly testified to the committee.[3]

Earlier that same day, the U.S. Department of Justice and FBI announced an operation that disrupted the infiltration of hundreds of U.S. routers and critical infrastructure networks by a major Chinese state-backed hacking group known as Volt Typhoon.[4]

Similarly, the FBI has led recent operations that have resulted in the takedown of multiple notorious ransomware gang websites and related IT infrastructure/servers, including LockBit and AlphV/BlackCat.[5]

***2. The ONCD report expands the Biden administration's intense focus on software development — and specifically, software manufacturers — in order to combat these ever-increasing cyberthreats.***

In May 2021, the Biden administration launched a concerted initiative with the specific objective to impose greater accountability and liability on software developers that develop

products with allegedly inadequate attention to product cybersecurity.

This effort began with U.S. President Joe Biden's 2021 Executive Order No.14028 on cybersecurity, and has been elaborated on and further intensified more recently as part of the White House National Cybersecurity Strategy and its implementation plan — both released in 2023 — and the many public statements by CISA, ONCD and other government officials over the last two years.[6]

The ONCD report released at the end of February further adds to this vision.

It's important to note that, shortly after the ONCD report was published, CISA approved a secure software development attestation form that requires software developers working with the federal government to attest to certain secure software development practices — such as building software in a "secure environment," making a "good-faith effort to maintain trusted source code supply chains," and employing "automated tools" to "check for vulnerabilities."[7]

Pursuant to a memo by the Office of Management and Budget, federal agencies can only use software from developers that have attested to using secure development practices beginning in the next three or six months, depending on the type of software.[8]

**The February 2024 White House ONCD Report**

With that framing, below are our three key takeaways from the ONCD report.

While self-described as a "technical" document, the ONCD report contains important information that nontechnical people should be well aware of and understand. Indeed, readers should take account of the ONCD report, and its context, in order to understand the White House's expectations on software security and to be alert to efforts by the administration to shift liability with or without requisite legislation or rulemaking.

Tech companies and software developers should also be sure to discuss the ONCD report's implications with in-house product security experts.

***1. Potential Liability***

First, the ONCD report lays new building blocks related to potential liability for software developers, including elements that could be used as a potential safe harbor threshold.

Shifting liability to software manufacturers has become a hallmark of the Biden administration's cybersecurity plan. To highlight one example: Last month, ONCD Director Harry Coker stated, "The [National Cyber] Strategy says we need to hold software manufacturers accountable when they rush insecure code to market: so, we're working with academic and legal experts to explore different liability regimes. We will soon be engaging with you to hear industry's perspective."[9]

The ONCD report furthers this agenda in two ways.

First, it advocates that software developers must only use "memory safe" programming languages to protect against certain types of vulnerabilities.

As background, memory safety refers to how computer memory can be accessed, written and allocated. In short, the type of programming language used to develop software

matters from a security perspective: Experts have identified certain programming languages, such as C and C++, that are susceptible to memory safety vulnerabilities, such as Morris Worm and Heartbleed.

As an overly simplified example, if a user asks software for a sixth item on the user's list of five items, the user should receive an error — but if the code was written in a language that is not memory safe, the software may pull information from a different source, i.e., out-of-bounds read, creating a security risk.[10]

The ONCD report clearly advocates that the use of memory safe languages should become the standard used by software developers.

And, taking a step back, this clearly begs a number of questions from a liability perspective: Will the use or nonuse of memory safe languages be incorporated into a future liability regime or safe harbor? Would legacy products that do not use memory safe languages be treated differently than new products developed in the future?

As the ONCD report acknowledges itself, "there are no one-size-fits-all solutions in cybersecurity;"[11] but the notion of safe versus unsafe programming languages certainly begins to feel like a discussion about liability.

Second, the ONCD report also invites the technical community "to develop empirical metrics that measure the cybersecurity quality of software."[12] Put another way, develop a quantitative way to measure whether software is sufficiently secure or not.

As the White House acknowledges, this would be a shift in how cyber quality is measured: Today, it is a qualitative and static assessment of software code. This current method of review, however, is insufficient because it is primarily backwards looking; failing to provide insight into "future threats or attack vectors."[13]

The ONCD report continues: "If developed, robust software measurements could improve one's ability to evaluate cybersecurity quality."[14] The next logical step, although not explicitly stated in the ONCD report, is that any evaluation might become the foundation for a liability regime.

This could mean, for example, some degree of immunity for manufacturers that score above a certain threshold on the evaluation, and some degree of potential liability for software that scores below a lower threshold.

### *2. Broadened Responsibility*

Second, the ONCD report is broadening potential responsibility for software developers.

Specifically, the ONCD report attempts to shift what software developers must focus on regarding the security quality of software: Developers must consider not only software code itself, but also the "attack surface" when developing secure software products.[15]

By calling for a "proactive approach" that "reduces the potential attack surface," the U.S. government is pushing technology manufacturers to consider risks beyond just the code, and consider all paths for data and commands into and out of the application.[16] Taking this to the next logical step, this could signal a shift in what developers could be held accountable for — i.e., alleged failure to consider the entire attack surface in developing software.

As the ONCD report succinctly states: "Programmers writing lines of code do not do so without consequence; the way they do their work is of critical importance to the national interest."[17]

This concept of broad responsibility for software security is intertwined with two related areas that have garnered specific focus from CISA — open-source software and artificial intelligence.

1. On March 5 and 6, CISA held the two-day Open Source Software Security Summit convening community leaders and announcing key actions to help combat security flaws in the open-source ecosystem, such as the Log4Shell vulnerability in 2021.[18] For example, CISA is working closely with package repositories to foster adoption of the Principles for Package Repository Security.[19]

At the summit, Easterly noted:

> This [Secure by Design ("SBD")] campaign is a push for software manufacturers to build in security from the start, thereby taking more ownership of their customers' cybersecurity outcomes. How software manufacturers approach open source software is fundamental to SBD. We need companies to be both responsible consumers of and sustainable contributors to the open software they use. This means properly vetting their open source software.

2. In November 2023, CISA and the U.K. National Cyber Security Centre, along with 23 domestic and international cybersecurity organizations, released guidelines for securing AI system development.[20] The guidelines "provide essential recommendations for AI system development and emphasize the importance of adhering to Secure by Design principles."[21]

### *3. Accountability for Product Security*

Third, the Biden administration remains focused on holding senior management and boards of software companies accountable for the security of their products.

This is not a new point by the Biden administration, but rather the continuation of a key component of its view on cybersecurity: Senior management and boards are "ultimately accountable" for the cybersecurity quality of their products.

To give a few past examples of this focus:

- In a February 2023 article published in Foreign Affairs by Easterly and Executive Assistant Director for Cybersecurity Eric Goldstein, the CISA leaders warned against "creators [rushing] to release [software] to customers [that] are more often focused on feature expansion than security," and argued that "[p]roblems should be fixed at the earliest possible stage — when technology is designed rather than when it is being used. Under this new model, cybersecurity would ultimately be the responsibility of every CEO and every board."[22]

- A few months later, CISA joined the FBI, the NSA, and over a dozen international partners in an updated guidance on secure software development. They wrote: "While technical subject matter expertise is critical to product security, senior executives are the primary decision makers for implementing change in an

organization. Executives need to prioritize security as a critical element of product development across the organization, and in partnership with customers."[23]

- The U.S. Securities and Exchange Commission's complaint against SolarWinds and its CISO — SEC v. SolarWinds Corp. in the U.S. District Court for the Southern District of New York, amended in February — in part, alleges false and misleading public statements about its secure software development practices: "SolarWinds and [its CISO] knew, or were reckless or negligent in not knowing, that the Company was still working to determine how to incorporate aspects of an SDL [Secure Development Lifecycle] into its product development leading up to and throughout the Relevant Period."[24]

The White House ONCD report clearly reiterates the administration's focus on this point:

> Software manufacturers are not sufficiently incentivized to devote appropriate resources to secure development practices, and their customers do not demand higher quality software because they do not know how to measure it... . While the technical executives, like the CTO, CIO, and CISO, play a defining role in executing this vision, cybersecurity quality must also be seen as a business imperative for which the CEO and the board of directors are ultimately accountable.[25]

Additionally, the recently approved CISA secure software development attestation form mentioned above must be signed by the "CEO or Designee with authority to bind the corporation."[26] In light of CISA's focus on accountability, the individual signing the form may wish to consider the internal substantiation supporting the attestation.

**What's Next?**

The National Cybersecurity Strategy Implementation Plan calls on ONCD to host a legal symposium considering "different approaches to a software liability framework" by June 2024.[27]

The symposium has yet to be announced, but the administration indicated last fall that it was gathering input from academics and technical experts.

---

*Alan Charles Raul is a senior counsel and founder of the privacy and cybersecurity practice at Sidley Austin LLP.*

*Stephen McInerney is a senior managing associate at the firm.*

*Vishnu Tirumala is an associate at the firm.*



[1] Office of the National Cyber Director, Back to the Building Blocks: A Path Toward Secure and Measurable Software (Feb. 28, 2024), https://www.whitehouse.gov/wp-content/uploads/2024/02/Final-ONCD-Technical-Report.pdf ("ONCD Report").

[2] ONCD Report at 14.

[3] Press Release, The Select Committee on the CCP, Select Committee on CCP Holds Hearing on CCP Cyber Threat to American Homeland (Jan. 31, 2024) https://selectcommitteeontheccp.house.gov/media/press-releases/media-package-select-committee-ccp-holds-hearing-ccp-cyber-threat-american.

[4] Press Release, U.S. Dep't of Just., U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure (Jan. 31, 2024) https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical#:~:text=%E2%80%9CVolt%20Typhoon%20malware%20enabled%20China,is%20not%20going%20to%20tolerate.

[5] Press Release, U.S. Dep't of Just., U.S. and U.K. Disrupt LockBit Ransomware Variant (Feb. 20, 2024) https://www.justice.gov/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant; Press Release, U.S. Dep't of Just., Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant (Dec. 19, 2023) https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant.

[6] Exec. Order No. 14028, Executive Order on Improving the Nation's Cybersecurity, 86 Fed. Reg. 26633 (May 12, 2021) https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/; Office of the National Cyber Director, National Cybersecurity Strategy (Mar. 2023); https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf; Office of the National Cyber Director, National Cybersecurity Strategy Implementation Plan (Jul. 13, 2024), https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf ("Implementation Plan").

[7] CISA, "In Effort to Bolster Government Cybersecurity, Biden Administration Takes Step to Ensure Secure Development Practices" (Mar. 11, 2024), https://www.cisa.gov/news-events/news/effort-bolster-government-cybersecurity-biden-administration-takes-step-ensure-secure-development.

[8] OMB, "M-23-16: Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices" (Jun. 9, 2023), https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-16-Update-to-M-22-18-Enhancing-Software-Security-1.pdf.

[9] Remarks: National Cyber Director Coker Remarks at the Information Technology Industry Council Intersect Tech Policy Summit (Feb. 7, 2024), https://www.whitehouse.gov/oncd/briefing-room/2024/02/07/remarks-national-cyber-director-coker-remarks-at-the-information-technology-industry-council-intersect-tech-policy-summit/.

[10] Prossimo, What is memory safety and why does it matter? (2022), https://www.memorysafety.org/docs/memory-safety/.

[11] ONCD Report at 8.

[12] Id. at 11.

[13] Id. at 12.

[14] Id. (emphasis added).

[15] Id. at

[16] Id. at 5.

[17] Id. at 6.

[18] CISA, "CISA Announces New Efforts to Help Secure Open Source Ecosystem" (Mar. 7, 2024) https://www.cisa.gov/news-events/news/cisa-announces-new-efforts-help-secure-open-source-ecosystem

[19] Jack Cable and Zach Steindler, "Principles for Package Repository Security" (Feb. 2024) https://repos.openssf.org/principles-for-package-repository-security.

[20] "Guidelines for Secure AI System Development" https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development.

[21] CISA, "CISA and UK NCSC Unveil Joint Guidelines for Secure AI System Development" (Nov. 26, 2023) https://www.cisa.gov/news-events/alerts/2023/11/26/cisa-and-uk-ncsc-unveil-joint-guidelines-secure-ai-system-development.

[22] Jen Easterly and Eric Goldstein, "Stop Passing the Buck on Cybersecurity," Foreign Affairs (Feb. 1, 2023) https://www.foreignaffairs.com/united-states/stop-passing-buck-cybersecurity.

[23] Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software at 10 (Oct. 2023) https://www.cyber.gov.au/sites/default/files/2023-10/Principles-and-Approaches-for-Security-by-Design-and-Default-%28October-2023%29.pdf.

[24] Amended Complaint ¶ 115, SEC v. SolarWinds Corp., No. 23-cv-9518 (S.D.N.Y. Feb. 16, 2024), ECF No. 85.

[25] ONCD Report at 14.

[26] CISA, "In Effort to Bolster Government Cybersecurity, Biden Administration Takes Step to Ensure Secure Development Practices" (Mar. 11, 2024), https://www.cisa.gov/news-events/news/effort-bolster-government-cybersecurity-biden-administration-takes-step-ensure-secure-development.

[27] Implementation Plan at 30.