

# Supply Chain Security Guidance

for addressing President Biden's  
Executive Order on Improving  
the Nation's Cybersecurity

# If you think your software is secure, get ready to prove it.

On May 12, 2021, President Joe Biden released an Executive Order (EO) on improving the nation's cybersecurity. The President has directed several government agencies to begin formulating guidelines and rules to shape an environment where security is verifiably baked into technology products.

This EO directs these agencies to develop new security requirements for software vendors selling into the U.S. government. These requirements will be incorporated into federal contracts for commercial software and hardware with the intent of imposing "more rigorous and predictable mechanisms for ensuring that products function securely, and as intended." This is a monumental shift that will have an immediate impact on global software development processes and lifecycles.

In addition to a host of new information and operational security measures that government agencies need to implement, the new order establishes a robust approach to supply chain security. The new requirements will include security testing throughout the development process as well as a Software Bill of Materials (SBOM) to address security issues in open source components.

This EO will have a significant impact on:

- Software and firmware developers
- Chief Product Security Officers (CPSOs)
- IoT, Industrial Internet of Things (IIoT), and Operational Technology (OT) equipment manufacturers
- Medical device/IoMT manufacturers
- Aerospace and defense companies
- The U.S. Energy sector and other critical infrastructure

While this EO is targeted at federal procurement, we fully anticipate that other sectors will quickly adopt the requirements as embodying industry best practices – whether as part of their standard contracting language, in security questionnaires, or as prerequisites for cyber insurance coverage. Furthermore, the reach of U.S. Federal procurement is so vast, that we expect virtually all device manufacturers and software companies to be profoundly impacted.

**This document will provide a brief overview of the key Supply Chain Security components of the EO, what they mean for device manufacturers, and how the Finite State Platform addresses each challenge.**



The background is a dark blue gradient with a complex pattern of white and light blue circuit traces. Several padlock icons are scattered across the image, some in white and some in a lighter blue, appearing to be part of the circuitry or overlaid on it. The text is centered in the upper half of the image, with each word or short phrase on a separate orange rectangular background.

**“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.”**

*– Executive Order on Improving the  
Nation’s Cybersecurity, 2021*

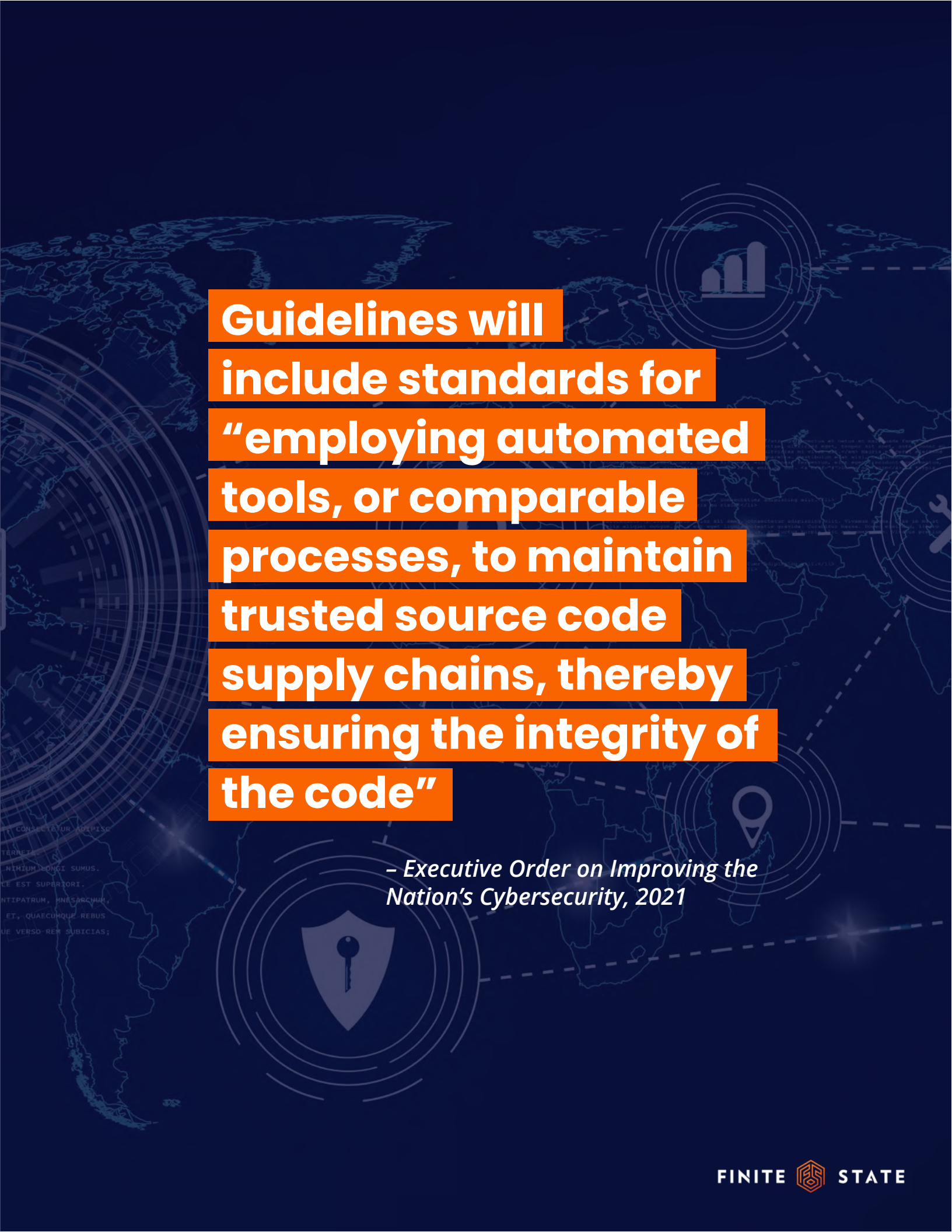
# Software and connected device vendors will need to start providing more proof of their products' security, their testing approach, vulnerabilities impacting their products, and their security development lifecycle.

Simply responding to a third-party risk questionnaire about high-level software development practices is no longer enough. Product security and engineering teams now need to provide an accurate and complete SBOM, detailed output from their security testing tools, assurances about their supply chain and development environment security, and detailed reports about the provenance of all of the components in their software.

## **We recommend that all developers of embedded device software:**

- Have an owner for product security (e.g. CPSO)
- Get tooling in place to determine an accurate inventory of all components in your product, including third-party software
- Implement automated, scalable testing and remediation processes throughout the development lifecycle
- Understand your suppliers and their supply chains, including having a comprehensive inventory of components and their vendors

*The Finite State Platform is an automated tool that allows your organization to test connected device firmware at scale. This will allow you to gain visibility into each component and its supply chain, identify vulnerabilities in your products, and give your team the actionable security guidance that they need to remediate risks.*



**Guidelines will include standards for “employing automated tools, or comparable processes, to maintain trusted source code supply chains, thereby ensuring the integrity of the code”**

*- Executive Order on Improving the Nation's Cybersecurity, 2021*



# Software and device vendors will need to prove that they protect their development environments and software supply chains from potential threats.

The most important step is to ensure that your engineering teams, development environments, and all source code are being secured in accordance with best practices for network and supply chain security in a comprehensive documented process.

What we can take away from SolarWinds is that software supply chains and development environments are attractive targets for malicious actors. One of the best countermeasures to potential compromise is to ensure that you have traceability from your final software build to the original source code and testing in place on those final builds.

To achieve that level of traceability, you need to comprehensively identify every first- and third-party component in your final software build and understand any changes that could have been introduced during the build process.

*The Finite State Platform provides full visibility into your software supply chains, including identifying all first-party, third-party, and open source components in your final build. Our massive intelligence repository ensures that you have the most up to date data on security risks and vulnerabilities associated with your software and/or suppliers. Static binary, program, and system testing, even the most subtle security issues can be detected before your software is shipped.*

**Guidelines will include standards for “employing automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them, which shall operate regularly, or at a minimum prior to product, version, or update release”**

*- Executive Order on Improving the Nation's Cybersecurity, 2021*

# Software and connected device vendors will need to employ automated testing tools to check for vulnerabilities in first- and third-party software, and those tools will need to be run against every product, version, and update release.

Software developers will need to adopt a robust security testing tool suite to ensure that the entirety of their products are being tested. In particular, this can be very challenging for connected device and embedded systems development environments.

These devices and their firmware tend to be built using custom build tools and processes that are incompatible with traditional Application Security tools. Additionally, most of the vulnerabilities in these devices manifest at the system level (e.g. misconfigurations of operating system services, embedded credentials, etc.), which requires new approaches for scalable security testing.

*The Finite State Platform is an automated tool built specifically for connected devices and embedded systems. It allows your team to test all device firmware, product versions, and updates at scale regardless of your team's existing development environments and build tools. With a combination of SAST, SCA, and static system testing, the Finite State Platform ensures that you achieve comprehensive, automated testing for first- and third-party vulnerabilities and misconfigurations, whether previously known or unknown, **every time** you build and ship your firmware.*



**“Guidelines will include standards for “providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website”**

**“...obtaining an SBOM, and using it to analyze known vulnerabilities are crucial in managing risk.”**

*- Executive Order on Improving the Nation's Cybersecurity, 2021*

# Software and connected device vendors will be required to provide a software bill of materials alongside every product that they sell to a Federal entity.

Most modern software is composed of numerous third-party and open source components rather than being written line by line. Assuring the security of software increasingly depends upon a developer's ability to produce an accurate and comprehensive list of all of those components. There are numerous open source and commercial tools available that can help with this problem, but it will also require an investment in people, processes, and training.

For connected devices, software composition analysis (SCA) can be particularly challenging due to the lack of transparency into your suppliers' software and lack of embedded development environment compatibility from traditional Application Security products. Finite State recommends that you seek an SCA solution that can operate on final firmware builds, identify components and dependencies within code and compiled binaries, and analyze software regardless of its underlying hardware/instruction set architecture. This will ensure that you can stand behind the accuracy and completeness of your SBOM.

*Manually producing an SBOM is a difficult process which tends to have error prone results. Finite State uses device-specific Software Composition Analysis (SCA) to produce a complete and accurate SBOM by analyzing your device firmware and creating a comprehensive list of device components. We do this on your final builds without requiring any changes to your build processes or access to your source code.*

**Guidelines will include standards for “providing, when requested by a purchaser, artifacts of the execution of the tools and processes [to secure code supply chains, check for vulnerabilities, and remediate them] and making publicly available summary information on completion of these actions, to include a summary description of the risks assessed and mitigated.”**

*- Executive Order on Improving the Nation's Cybersecurity, 2021*



# Software and connected device vendors will not only need to test their products — they will also need to provide testing results to their customers.

Trust and security require visibility, and this requirement opens up traditionally internal information to external stakeholders. It's important that software and connected device developers recognize that their security testing tools need to output reporting that's appropriate for consumption by their customers but proves the execution of a robust security process. **It's important to present this information in a transparent manner that:**

- accounts for nuances of the development processes
- allows for vendor commentary on any security issues identified, and
- summarizes the risk against industry benchmarks and standards.

*The Finite State Platform provides extensive, comprehensive, and customizable reporting that allows your team to share risk information with your customers, your leadership, and other key internal and external stakeholders.*

**Guidelines will include standards for “attesting to conformity with secure software development practices [and] ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion of a product**

*- Executive Order on Improving the Nation's Cybersecurity, 2021*

# In addition to conducting the required security testing and providing the requested data about your software and supply chains, each vendor will have to attest that their security practices are compliant with key security requirements and that all the data provided is accurate.

The direction from the EO is to push companies towards demonstrable compliance with security practices. As with other elements of the EO, simply checking a box on a security questionnaire will not be sufficient.

**Companies will need to affirmatively state that they have met specifically articulated security requirements.**

Software and connected device developers will need to have the utmost confidence in their product security program and associated artifacts that they share with their customers. This means that tooling needs to be robust, compatible with your entire product portfolio, and transparent in its processes.

While companies might be inclined to gloss over such requirements, a false attestation could result not only in termination of a specific contract, it could lead to an investigation by the relevant agency's inspector general and the possibility of being blocked from doing business with the federal government.

*The Finite State Platform provides a comprehensive view of the overall security of your products and their supply chains, giving you the information you need to attest to the integrity of your product security. Because Finite State tests your final build, you can stand behind the results with confidence and know that you have fully tested what you're actually shipping to your customers.*



# What does a comprehensive product security program look like?

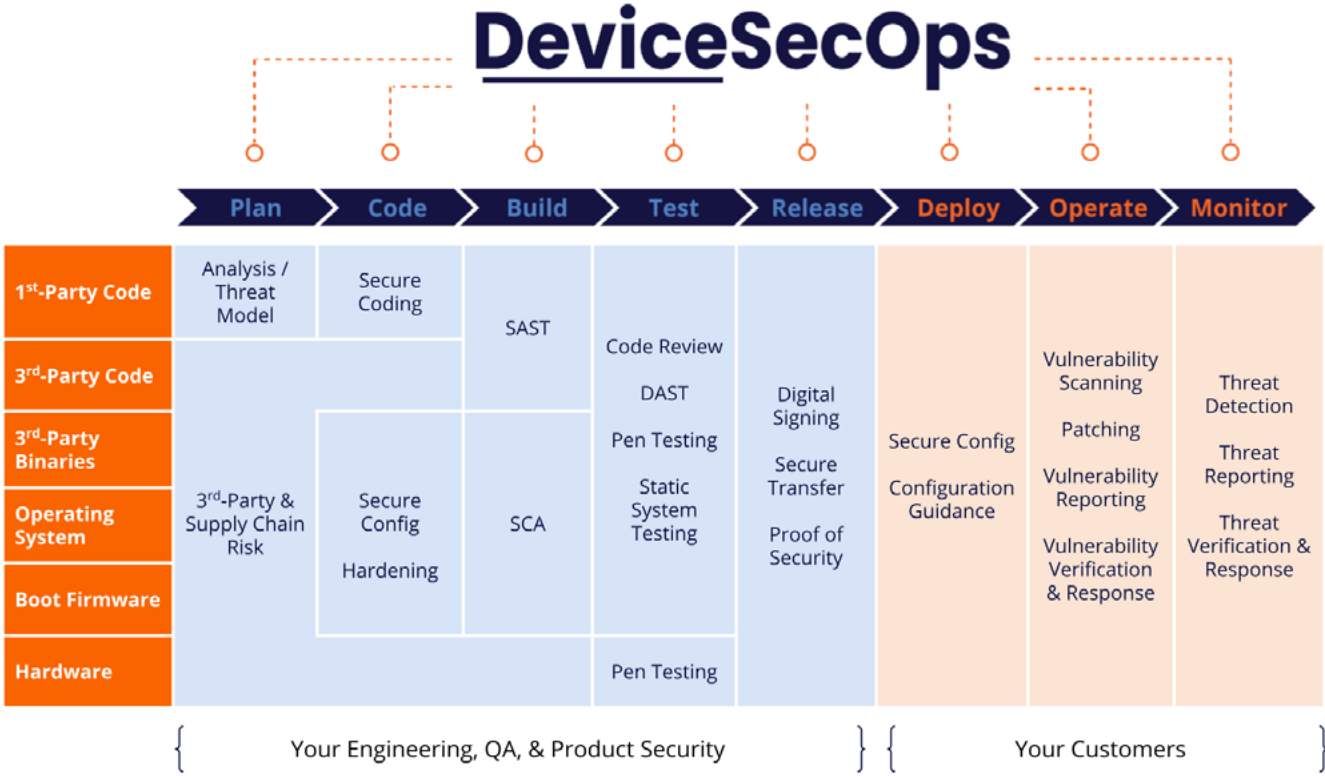
Analyzing device firmware requires an approach that tests an entire system made up of hundreds of programs, including drivers, applications, and operating systems. The only way to truly understand what's in your device is to use tools that were built specifically to handle the complex file formats, system configurations, binaries, and processor architectures found within these devices.

Due to this complexity, it's more crucial than ever to test every build of your firmware early and often in the development lifecycle and remediate vulnerabilities as quickly as possible. Employing an automated tool built specifically for analyzing device firmware removes a huge part of that burden from your development and security teams, allowing them to focus on remediating security

issues and mitigating supply chain risk.

At a minimum, your tools should utilize Software Composition Analysis (SCA), Static Application Security Testing (SAST), and Static System Testing in order to analyze your device firmware and provide you with an accurate inventory of your components. Additionally, your team must be able to see and ensure that your products are securely configured in order to remove potential backdoor vulnerabilities.

The graphic below provides an overview of the testing and processes needed at each stage of the development lifecycle in order to ensure the security of your products.



# How do Finite State's capabilities map to the new EO requirements?

Though the specific requirements outlined in the EO have yet to be formally written, here are the ways your organization can leverage to Finite State Platform to prepare for the anticipated requirements:

EO Directive	Meaning	Relevant Finite State Platform Capabilities
<p>"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."</p>	<p>Software and hardware vendors will need to start providing more proof of their products' security, their testing approach, vulnerabilities impacting their products, and their security development lifecycle.</p>	<ul style="list-style-type: none"> <li>• SCA, SAST, and static system testing capabilities</li> <li>• Accurate and complete SBOM</li> <li>• Known CVEs, legal and licensing risk, and configuration vulnerabilities</li> <li>• Comprehensive, shareable reporting</li> </ul>
<p>Guidelines will include standards for "employing automated tools, or comparable processes, to maintain trusted source code supply chains, thereby ensuring the integrity of the code"</p>	<p>Software and device vendors will need to prove that they protect their development environments and software supply chains from potential threats.</p>	<ul style="list-style-type: none"> <li>• Accurate and complete SBOM</li> <li>• Testing of final builds of software and firmware, not just source code</li> <li>• Traceability of final builds back to the original components</li> <li>• Comprehensive vulnerability detection</li> </ul>
<p>Guidelines will include standards for "employing automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them, which shall operate regularly, or at a minimum prior to product, version, or update release"</p>	<p>Software and connected device vendors will need to employ automated testing tools to check for vulnerabilities in first- and third-party software, and those tools will need to be run against every product, version, and update release.</p>	<ul style="list-style-type: none"> <li>• Scalable, automated firmware analysis that can be easily incorporated into your DevSecOps process without changing your existing tooling</li> </ul>

EO Directive	Meaning	Relevant Finite State Platform Capabilities
<p>Guidelines will include standards for “providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website” “... obtaining an SBOM, and using it to analyze known vulnerabilities are crucial in managing risk.”</p>	<p>Software and connected device vendors will be required to provide a software bill of materials alongside every product that they sell to a Federal entity.</p>	<ul style="list-style-type: none"> <li>• Accurate and complete SBOM</li> <li>• Automated platform that allows your organization to produce SBOM and supply chain risk reports at scale, without changing your development environment or tooling</li> </ul>
<p>Guidelines will include standards for “providing, when requested by a purchaser, artifacts of the execution of the tools and processes [to secure code supply chains, check for vulnerabilities, and remediate them] and making publicly available summary information on completion of these actions, to include a summary description of the risks assessed and mitigated”</p>	<p>Software and connected device vendors will not only need to test their products — they will also need to provide testing results to their customers.</p>	<ul style="list-style-type: none"> <li>• Comprehensive, shareable reporting</li> </ul>
<p>Guidelines will include standards for “attesting to conformity with secure software development practices [and] ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion of a product”</p>	<p>In addition to conducting the required security testing and providing the requested data about your software and supply chains, each vendor will have to attest that their security practices are compliant with key security requirements and that all the data provided is accurate.</p>	<ul style="list-style-type: none"> <li>• Testing of final builds of software and firmware, not just source code</li> <li>• Traceability of final builds back to the original components</li> <li>• Supply chain risk report</li> <li>• SBOM tied to publicly reported vulnerabilities (CVEs) and third party risk information</li> <li>• Comprehensive, shareable reporting</li> </ul>



# The world ahead

Ultimately, this executive order signals a new era for cybersecurity that puts regulators, developers and manufacturers, and the larger cybersecurity community firmly on the same page, speaking from the same playbook. It empowers security professionals to act with confidence and organizations to build out their security infrastructure to support their needs. The end result will be a safer, more secure national ecosystem that holds all of us accountable.

## Additional Resources:

### Managing Open Source Risk for Connected Devices

Open source software, libraries, and operating systems aid in the efficiency of the product development process. They've also increased the risk of security and licensing issues for those products. Finite State has made it easy to manage open source risk for connected devices, such as the Internet of Things (IoT), industrial control systems (ICS), connected medical devices (IoMT), and the industrial internet of things (IIoT).

<https://finitestate.io/open-source-risk-connected-devices>

### Device manufacturers need to rethink how to lock down IoT

As the number of IoT and embedded devices increases, device manufacturers must radically rethink their approach to product security. Finite State CEO, Matt Wyckhouse, discusses how to meet the demands of this emerging digital world for SC Magazine.

<https://finitestate.io/articles/sc-magazine/device-manufacturers>

### Finite State Supply Chain Assessment: Huawei Technologies

Amidst the proliferation of connected devices, 5G security has been a pressing topic in cybersecurity. In June of 2019, Finite State released a report revealing numerous vulnerabilities and backdoors in Huawei 5G networking devices.

<https://finitestate.io/2019/06/27/huawei-supply-chain-assessment>

 @FiniteStateInc

 /company/FiniteState

 [www.finitestate.io](http://www.finitestate.io)