CYBELLUM

Product Security Takeaways from the

National Cybersecurity Strategy 2023

Table of Contents

Opening Letter

Uncle Sam is stepping up to the cyber plate.

He's been talking a big cybersecurity game over the last couple of years, letting industries, such as automotive, medical device, critical infrastructure, and others know that the days of the internet wild-west are coming to an end.

This Product-Security review of the White House National Cybersecurity Strategy 2023 reads between the lines, extracting the key points manufacturers need to consider today if they want to keep their devices in the field tomorrow.

Despite staying away from naming any specific actions, there was one exception: The SBOM

Acting as a critical piece for the growing product security sector, the SBOM seems to have become the Federal Government's foundation for any future regulation. Without managing this critical list of software ingredients for each device, protection and compliance isn't scalable.

The Biden administration has made clear how it's ready to activate every branch of the Federal Government in order to tackle our poor cybersecurity reality. Their goals will rest on five strategic pillars- each with their own focus.

Harking back to waking the sleeping giant in 1942, America is ready to take action against foreign threats in the cyber arena. Calling out specific countries for their breaches, the US government is ready to lead the cybersecurity charge– with the precision required to ensure national security.

Part 1:

The big picture

It's no secret that the internet has become the new wild-west.
However, this time, instead of romanticized Robinhood-style cowboys, we have nation-states funding terror activities and laundering money through cyber crimes. Unpatrolled, companies are faced with imminent strikes and individuals are sitting ducks for a targeted bad-actor.

President Biden opens the White House Cybersecurity Strategy 2023 with a clear message, setting the tone for the rest of the document, “We need to be able to trust that the underlying digital ecosystem is safe, reliable, and secure.” As we have seen before, the United States is always ready to invest resources to protect its most prized assets— the economy.

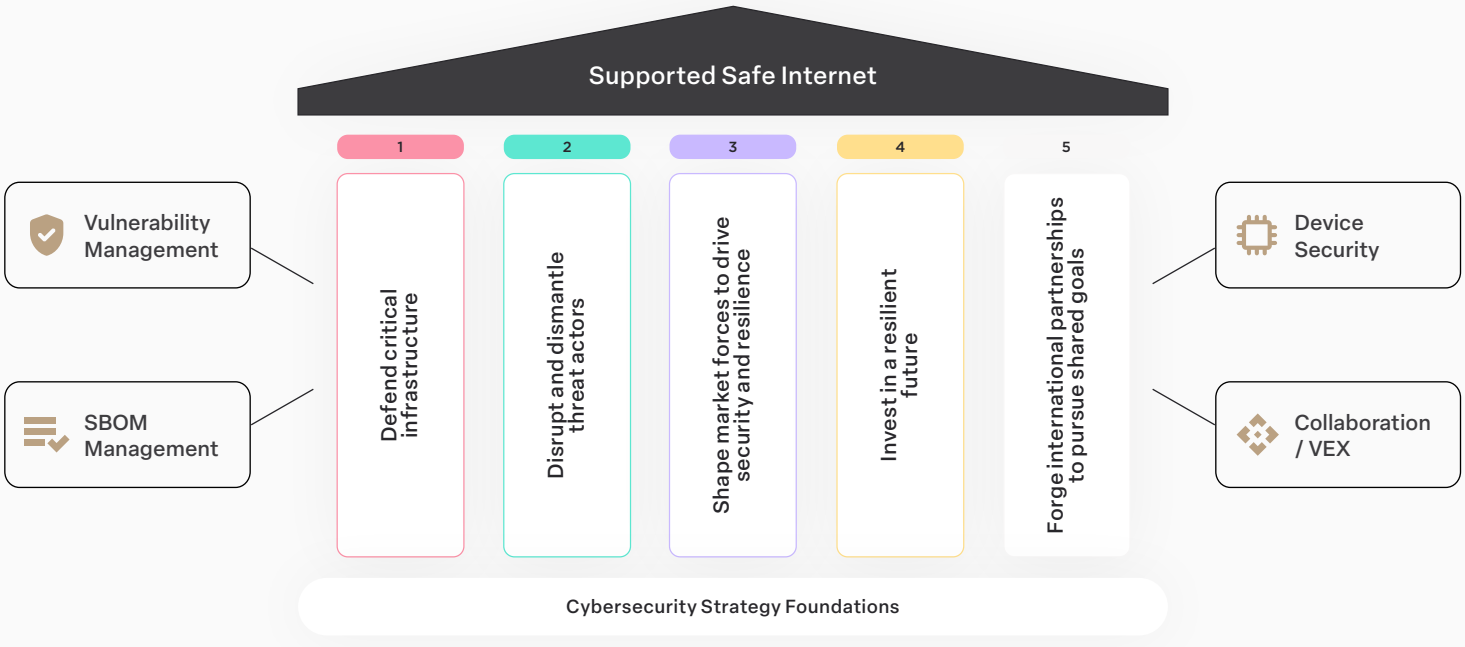
Critical for Chief Product Security Officers (CPSOs), this document follows EO14028, giving us guidelines on what future cybersecurity practices will look like, and the December 2022 Omnibus bill that offers the funding for EO14028. For anyone sitting at a critical infrastructure juncture, this strategy gives 5 pillars that it will use to ensure a secure internet for the US and its allie’s.

They are:

Pillar 1: Defend critical infrastructure
Pillar 2: Disrupt and dismantle threat actors
PIllar 3: Shape market forces to drive security and resilience
Pillar 4: Invest in a resilient future
Pillar 5: Forge international partnerships to pursue shared goals

While at first this may seem like yet another piece of regulation to follow, the Biden administration appoints various agencies to specialized roles, staying away from implying specific legislation.
On the other hand, the government is ready to invest in those who need help bolstering their product security protection, such as medium to small manufacturers and software supply chain vendors.
It even said that it is willing to shield them from future liability if they follow development guidelines.

5 Pillars of the White House Cybersecurity Strategy 2023



Part 2:

What's in the strategy?

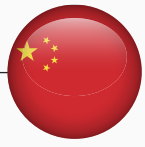
Manufacturers, and the vendors who supply them are faced with rising pressure from all sides.

On the one hand, CPSOs know they need to protect their devices and have made great strides towards security over the last few years. On the other hand, there are budgetary restraints, growing regulatory procedures, hazardous supply chains, and real-time cyber threats to be addressed. This document reads out as a call to congress, shouting 'they don't need more regulation, they need action!'

Looking to approach protecting the free internet as a public-private venture, the Federal Government looks the tech sector dead in the eye– aware of how delicate the systems we've built really are. "Software and systems are growing more complex, providing value to companies and consumers but also increasing our collective insecurity. Too often, we are layering new functionality and technology on already intricate and brittle systems at the expense of security and resilience. The widespread introduction of artificial intelligence systems– which can act in ways unexpected even to their own creators– is heightening the complexity and risk associated with many of our most important technological systems."

The strategy then takes a birds-eye view of the situation, acknowledging that it's not fair or even possible for businesses or individual citizens to obtain the resources needed to protect themselves. Modern threats, often coming from abroad, are not only a threat to citizens, but a threat to national security.

The strategy specifically calls out four nations, each of which have used the internet as a way to attack critical infrastructure such as power, water, medical facilities, and more– putting lives in danger.
They are:



China

The document states that China is a surveillance state, "exporting it's vision of digital authoritarianism"

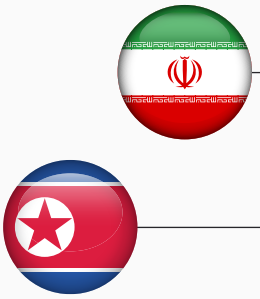
"The People's Republic of China (PRC) now presents the broadest, most active, and most persistent threat to both government and private sector networks and is the only country with both the intent to reshape the international order and, increasingly, the economic, diplomatic, miliary, and technological power to do so."

Russia

The Biden administration blames Russia for the "irresponsible spillover" that harms infrastructure and citizens across Europe as a result of the war in Ukraine.

"For more than two decades, the Russian government has used its cyber capabilities to destabilize its neighbors and interfere in the domestic politics of democracies around the world. Russia remains a persistent cyber threat as it refines its cyber espionage, attack, influence, and disinformation capabilities to coerce sovereign countries, harbor transnational criminal actors, weaken U.S. alliances and partnerships, and subvert the rules-based international system."

Iran and North Korea



Iran, which is under heavy sanctions for its nuclear program by the United States, has become increasingly comfortable working with North Korea. Helping one another track people and fund terrorist regimes.

“Iran and the Democratic People's Republic of Korea (DPRK) are similarly growing in their sophistication and willingness to conduct malicious activity in cyberspace. Iran has used cyber capabilities to threaten U.S. allies in the Middle East and elsewhere, while the DPRK conducts cyber activities to generate revenue through criminal enterprises, such as through the theft of cryptocurrency, ransomware, and the deployment of surreptitious information technology (IT) workers for the purposes of fueling its nuclear ambitions.”

Part 3:

The 5 pillars

Across the 5 pillars laid out by the administration, there are two beacons that are followed to regain a balance of responsibility and incentivise long-term security investments instead of short-term gains.

1. "We must defend the systems we have now, while investing in and building toward a future digital ecosystem that is more inherently defensible and resilient."

2. To achieve these goals, the Federal Government will focus on points of leverage throughout the supply chain to implement minimally invasive actions, (such as SBOM management) to produce the greatest gains in defensibility and systemic resilience.

The United States government is openly offering to protect companies against liability for what can be a potential financial risk.

Pillar 1: Defend critical infrastructure

Your network is secure, how about the devices that operate on it?

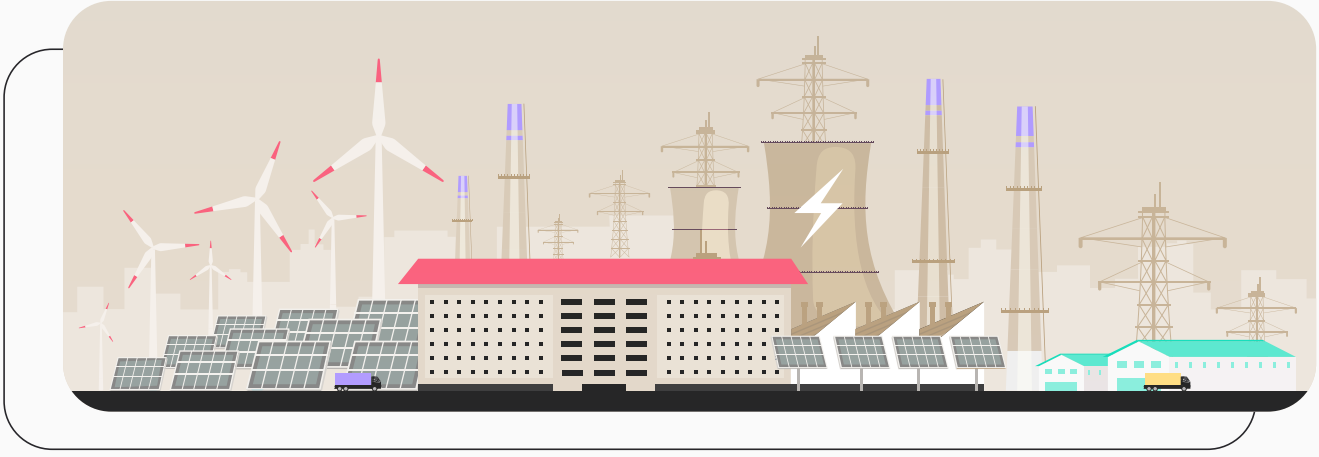
Our infrastructure has changed significantly over the last decade. Switching from upgraded versions of old technologies, companies across industries began integrating monitors, sensors, and IoT devices into people's most critical devices– each with their own software and digital supply chains. The United States has hundreds of independent utility operators, choosing solutions that promise to layer and protect state of the art devices onto legacy systems.

"We are building a smart grid, powered by distributed renewable electricity and balanced with intelligent systems that promises a bright and resilient future of energy abundance. We envision a maturing Internet of Things (IoT), comprising everything from consumer goods to digitized industrial controls to constellations of satellites, that will increase efficiency and safety while providing game-changing insights into our environment and economy. We are laying the foundations for real-time global collaboration leveraging vast amounts of data and computing power that will unlock scientific discoveries and other public goods of which we cannot yet conceive. Achieving this vision of a prosperous, connected future will depend upon the cybersecurity and resilience of its underlying technologies and systems."

While we speak of the dreams of what devices can do for humanity, our internet today remains a patchwork of various levels of security creating opportunities for threat actors to channel into a network via an authorized device, regardless of the level of security you've implemented.

Despite the government and its agencies' pushes to institute better cybersecurity practices, frustration remains. "While voluntary approaches to critical infrastructure cybersecurity have produced meaningful improvements, the lack of mandatory requirements has resulted in inadequate and inconsistent outcomes. Today's marketplace insufficiently rewards– and often disadvantages– the owners and operators of critical infrastructure who invest in proactive measures to prevent or mitigate the effects of cyber incidents. Regulation can level the playing field, enabling healthy competition without sacrificing cybersecurity or operational resilience."

While specifically stating that the private sector can handle most incidents on its own, there are times that companies will need to call upon the Federal Government for help. This is acknowledged in pillar one's Strategic Objective 1.3: Integrate Federal Cybersecurity Centers and Strategic Objective 1.4: Update Federal Incident Response Plans and Processes.



Software-driven devices layered on legacy systems create opportunities for security gaps.

Relying on a strong and ongoing public- private alliance, with the full Federal Government's support has worked before. After all, the Federal Government can go outside CISA at times to address cybersecurity issues. The TSA and EOA have yielded successful results with oil and natural gas pipelines, aviation, and rail led by the Transportation Security Administration and water systems, as well as by the Environmental Protection Agency. "The Federal Government must provide clear guidance on how private sector partners can reach federal agencies for support during cyber incidents and what forms of support the Federal Government may provide."

The strategy envisions all relevant branches of the Federal Government working directly with industry experts

Not only does this allow for more transparent communication, it would also allow the government to more quickly assist the private sector when needed. Agility must be a natural part of preparing regulations that reflect steps towards secure growth.

Pillar 2: Disrupt and dismantle threat actors

Pillar two lays out how America will work together with allies around the globe to either dismantle cyber criminal organizations or disrupt them to the point that their activities are no longer worthwhile.

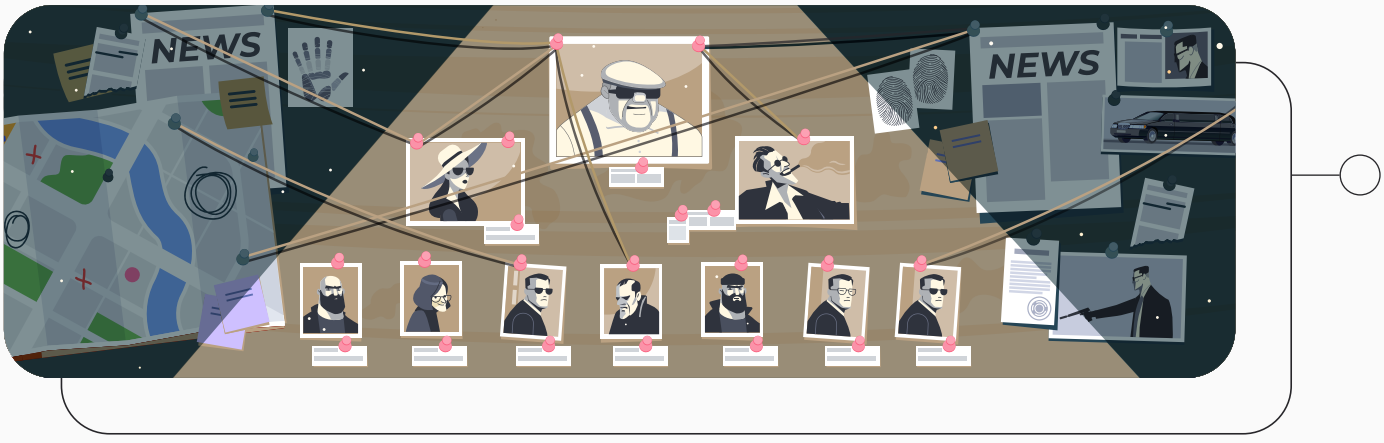
Below is an outline of what the government will be responsible for, what the private sector will be responsible for, and how to scale communication.

Strategic Objective 2.1: Integrate Federal Disruption Activities

This section makes clear what the government is willing to be responsible for.

"Disruption campaigns must become so sustained and targeted that criminal cyber activity is rendered unprofitable and foreign government actors engaging in malicious cyber activity no longer see it as an effective means of achieving their goals."

Product security response teams are uniquely positioned to be ready for any scenario. Examples can be rapidly patching a vulnerability, swapping a component, or even deciding to drop a potentially risky supplier who can't be accountable to reduce software supply chain risk. SBOMs allow us to immediately pinpoint across an entire fleet where the specific hazardous component exists. What would log4j have been like if everyone knew how to identify exactly which devices had this exact vulnerabilty?



Objective 2.1 explains how the Federal Government will disrupt threat actors and the agencies who support them.

Just a couple of weeks after releasing this strategy, CISA announced the Ransomware Vulnerability Warning Pilot (RVWP), aimed at updating companies on new ransomware incidents and releasing mitigation procedures. However, this is putting a bandaid on a wound, not addressing the cause of damage.

While the government will go after the threat actors, private organizations must look inward and ask if they are doing all they can to deter attackers by minimizing vulnerabilities before deployment and if they are ready to take in RVWP data and turn it into action.

Strategic Objective 2.2: Enhance Public-Private Operational Collaboration to Disrupt Adversaries

Acknowledging the private sector's ability to respond to market demands, this section lays out responsibilities that will keep processes agile.

> **The private sector has growing visibility into adversary activity. This body of insight is often broader and more detailed than that of the Federal Government, due in part to the sheer scale of the private sector and its threat hunting operations, but also due to the rapid pace of innovation in tooling and capabilities.**

This is not to say that the private sector will be able to act in a care-free manner. Working with the Federal Government now requires a device-specific SBOM to be provided along with the delivery of any equipment. Companies who are ready to be brought under the umbrella of protection offered by federal agencies must also be prepared to offer comprehensive and up to date SBOMs that reflect what lies inside each product, model, variation, and even each software component. As well intentioned as this may be, companies must acknowledge that managing a growing amount of SBOMs across all components and versions is proving to be quite a challenge, requiring a proper SBOM management strategy if they want to comply.

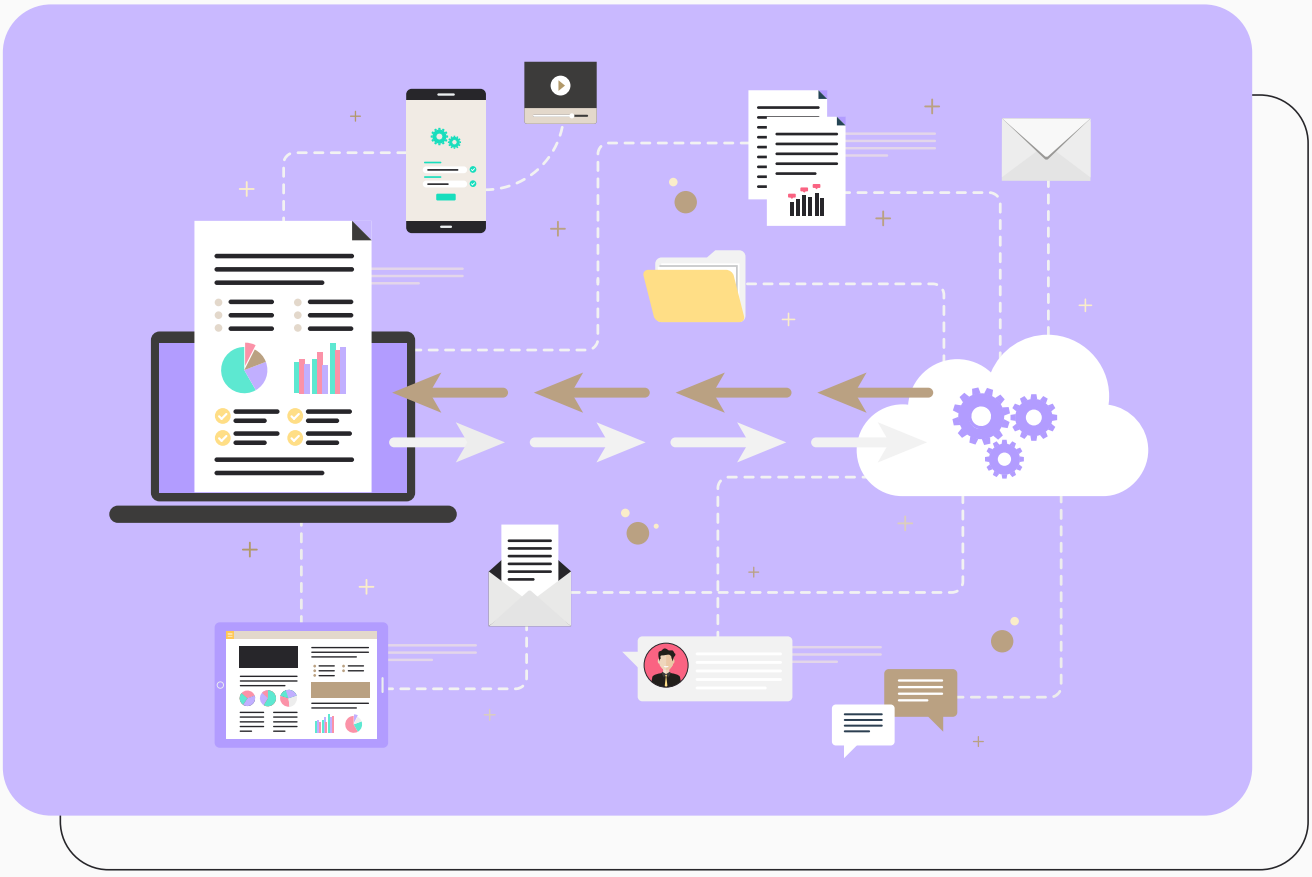
Strategic Objective 2.3: Increase the Speed and Scale of Intelligence Sharing and Victim Notification

Section 2.3 reminds both federal agencies and private businesses exactly who this strategy is for— the people. Whether providing internet service, power, transportation, medical care, or any other vital product or service, any impacted end user must be informed.

However, due to various channels and protocols, a customer may not know that a vulnerability or active threat applies to them until weeks or months after it has been discovered. After so much time, undoing any damage puts greater strain on resources, unfairly harming customers. To address this, the government will work on better communication by reviewing its policies and communication red tape.

"The Federal Government will increase the speed and scale of cyber threat intelligence sharing to proactively warn cyber defenders and notify victims when the government has information that an organization is being actively targeted or may already be compromised."

This brings up critical questions for CPSO's who are responsible for addressing post-deployment product security threats. "The Federal Government will also review declassification policies and processes to determine the conditions under which extending additional classified access and expanding clearances is necessary to provide actionable intelligence to owners and operators of critical infrastructure." Information coming from the Federal Government will include actionable procedures, however, if you are already compromised, swift action must be taken.



Actionable intelligence demands dialogue and insights between private operators and government offices.

2021's Log4j vulnerability caught teams off guard due to a lack of documentation and transparency. Having retooled IT security products instead of ones designed for product security, teams had to first begin searching throughout all of their business units and product lines to see where within their systems these software components existed– if at all.

To prevent this from happening again, a product security platform must be used to generate and manage SBOMs from the beginning of development throughout its full lifecycle. The Product Security platform can then automatically submit SBOMs for approval that were auto-generated during production as part of the product security workflow.

With a platform designed to protect devices, automation tools can support Product Security Incident Response Teams (PSIRT) and their efforts. Automatic vulnerability assessments, malware assessments, and other tools can identify which components are affected by rapidly matching vulnerabilities against an SBOM repository.

Once matched, PSIRTs can notify product owners, operators, and end-users about new vulnerabilities and recommended mitigation steps.

Pillar 3: Shape market forces to drive security and resilience

Not only does this pillar introduce the SBOM, it is worth noting that it is the only actionable method mentioned throughout the entire strategy. This is only one of the reasons why the third pillar is the most significant for manufacturers and Tier-N suppliers of connected devices.

A second reason is that it calls out poor practices that kick the proverbial product security can down the road. If only a small fraction of Tier-1 and 2 suppliers have lackluster product security processes, their poor security methods will find their way into countless vehicles, medical devices, industrial equipment, and other systems that are mission critical. Taking it further, if manufacturers don't have the most up-to-date list of all software components, then the vulnerability may go unnoticed and become introduced to end users.

The Cybersecurity Strategy 2023 looks to stop these poor security practices while galvanizing the cybersecurity community towards better collaboration.

> **To further incentivize the adoption of secure software development practices, the Administration will encourage coordinated vulnerability disclosure across all technology types and sectors; promote the further development of SBOMs; and develop a process for identifying and mitigating the risk presented by unsupported software that is widely used or supports critical infrastructure.**

Strategic objective 3.1: Hold the Stewards of Our Data Accountable

Taking a different perspective, the government understands that we won't be able to 100% trust our devices, if we can't trust the channels in which the data must traverse.

Looking to both international and domestic organizations, this document puts companies in the spotlight holding them accountable, stating "While market forces remain the first, best route to agile and effective innovation, they have not adequately mobilized industry to prioritize our core economic and national security interests." It later continues, "When organizations that have data on individuals fail to act as responsible stewards for this data, they externalize the costs on everyday Americans."

Addressing such poor practices will be achieved in two ways. One is to rely on NIST guidelines, limiting what data can be collected. The second this will be achieved through better practices in our product security.

Strategic Objective 3.3: Shift Liability for Insecure Software Products and Services

Throughout the strategy it mentioned that companies are rewarded for poor product security. Small and medium companies that don't have internal product security teams are rewarded for not investing resources in proper product security, instead choosing to address problems as they arise in the field.

"Markets impose inadequate costs on– and often reward– those entities that introduce vulnerable products or services into our digital ecosystem. Too many vendors ignore best practices for secure development, ship products with insecure default configurations or known vulnerabilities, and integrate third-party software of unvetted or unknown provenance. Software makers are able to leverage their market position to fully disclaim liability by contract, further reducing their incentive to follow secure-by-design principles or perform pre-release testing."

This is an incredible step, allowing the government to flip the script and tell companies that they are not responsible for their products, even if a contract is signed that is meant to absolve the supplier of any wrongdoing.

Following federal cybersecurity guidelines can help companies be approved for federal protection, even if a breach were to occur as a result of their product.

To benefit from this, suppliers and manufacturers will have to recognize that shipping products that contain known vulnerabilities is not an acceptable practice. If they want to be taken seriously by the Federal Government and reap the rewards that come with it, they will need to address all known vulnerabilities in their software before being delivered to customers.

However, it must also be acknowledged that many companies today lack the tools to conduct some of the practices outlined, either due to lack of funding, awareness, or proper product security driven tools.

In response, the strategy will push for the creation of a protection program where companies that follow government guidelines will be rewarded by protection from liability. "To begin to shape standards of care for secure development, the Administration will drive the development of an adaptable safe harbor framework to shield from liability companies that securely develop and maintain their software products and services."

The United States government is openly offering to protect companies against liability for what can be a potential financial risk, going as far as suggesting a federal cyber insurance backstop to help stabilize a company or the economy, should a major attack occur.

Strategic Objective 3.5: Leverage Federal Procurement to Improve Accountability.

The US is ready to sway market forces as a means to achieve its goals. In this pillar we are told "To build the secure and resilient future we want, we must shape market forces to place responsibility on those within our digital ecosystem that are best positioned to reduce risk.
We will shift the consequences of poor cybersecurity away from the most vulnerable, making our digital ecosystem more worthy of trust."

Today, e-commerce is a significant sector but what will digital commerce look like in the coming years as manufacturer's of connected devices bring subscription services to physical goods? Increased features being put behind paywalls, industry 4.0 increasing their reliance on autonomous devices, and the medical device industry continuing to connect their machines for greater monitoring, means that the Federal Government will apply increased pressure on companies to manage SBOMs and have them ready for action, should an incident occur.

While applauding the impact and progress brought upon by EO14028, this objective looks to use private-public product procurement to take it further.

Pillar 4 & 5: Partnerships and resilience

The last two pillars lay out resources, including international agreements and collaborative strategies that the Federal Government will invest.

The White House Cybersecurity Strategy in Action

Knowledge sharing

Better collaboration between private organizations as well as the government.

Ecosystem focused

Changing from increased regulation to driving market forces towards a common goal will be more simple within a flourishing ecosystem.

Accountability

Each vendor will be responsible for delivering a secure product. In addition, each manufacturer will ensure that the component is secure on its own and as part of the greater system.

Everyone doing their part

As covered in pillar two, various responsibilities will fall on the public sector while others will fall on the private sector. Each side will need to make good on their responsibilities if the strategy is to be successful.

Pillar 4: Invest in a resilient future

While news of breaches make the headlines nearly daily, the strategy found it important to say that it is actively intervening to prevent attacks from individual players, hacking groups, and state-backed hacking organizations. “Every day, cyber defenders foil state-backed attacks and prevent criminal plots around the world. But the underlying structural dynamics of the digital ecosystem frustrate their efforts. Its components remain prone to disruption, vulnerable to exploitation,
and are often co-opted by malicious actors.”

Investing in these five pillars is not only about addressing the problems of today but to lay the groundwork for protection into the future.

Pillar 5: Forge International Partnerships to pursue shared goals

As powerful and determined as the US government is to secure the nation’s cybersecurity and product security standing, the internet relies on a global system that can not be managed or patrolled by one nation.

That’s why partnerships with countries in North America, South America, Europe, and Asia is critical in ensuring America’s security. “The United States seeks a world where responsible state behavior in cyberspace is expected and rewarded and where irresponsible behavior is isolating and costly. To achieve this goal, we will continue to engage with countries working in opposition to our larger agenda on common problems while we build a broad coalition of nations working to maintain an open, free, global, interoperable, reliable, and secure Internet.”

Are SBOMs really the key?

This strategy, published by the Biden administration, outlines bold moves to stop lacking product security practices, reduce response times, and create a more trustworthy internet.
At the heart of all of this strategy is the expectation that we will know which software components exist within each device in real time. With a properly generated and managed SBOM system, companies automatically become more transparent and shave critical time in finding mitigations to some of today's most critical strategies.

The private sector will use SBOMs to identify and contain the spread of malicious software while the government will use it to keep vendors accountable, inform impacted parties of direct threats, and ensure that no vulnerabilities enter government systems.

Ultimately, the strategy demands that congress act to use SBOMs as the foundation of America's product security future, allowing domestic products to be looked at with the utmost trust. CPSOs are tasked with ensuring it streamlined product security processes from a managerial level and up keeping the high level of security expected of them.

> **Software Bills of Materials are a foundational single source of truth.**
>
> *Slava Bronfman, Co-Founder & CEO, Cybellum*

Time will tell if these companies are ready to partake in the future of secured device security– because if one thing is clear, it's that the future of America's products will be secured and companies must be ready if they are to compete.

More on SBOMs

SBOM for Connected Devices: Getting it Right

Cyber BOM and SBOM Management

SBOM & VEX Minimum Requirements

Cybellum, where teams do product security

Above trying to understand and manage all of the premarket guidelines, postmarket requirements, executive orders, and industry-specific standards, someone has to actually manage and oversee all aspects. To reduce pressure on security teams and enable them to perform tasks that are already nearly impossible to manage at scale, a dedicated product security solution is required.

SBOM Management

To comply with internal and external policies, SBOMs need to be verified, tracked, and approved for each product, component, and version, across multiple teams including development, QA, compliance, and of course security....

Cybellum automates the entire SBOM management process, so you go from detection to approval and vulnerability management in no time.

Manage all SBOMs in one place - Gain deep visibility into your supply chain, 3rd party software components, and proprietary code across components, products, and business units.

Track SBOM versions through time - Create and manage SBOMs continuously with every new version, and see the changes through time.

Make compliance much easier - Create, validate and generate reports quickly, so you easily meet industry standards from the likes of the FDA, ISO and others.

Integrate SBOM generation into existing workflows - Seamless integrations with your existing system such as PLM, CI/CD, and software update systems, and support for all SBOM and VEX format, such as CycloneDX and SPDX, including import and export.

Beyond simple SBOMs - Expose all associated risks beyond the simple SBOM, such as HW BOM, cryptography, passwords, PII, OS configuration, and more.

Focus more on security research, less on SBOM validation - without the costly and time consuming hassle of manual audits, you will be able to focus your time where it counts, on reducing risk and remediating critical vulnerabilities.

Audit-ready: Compliance-ready SBOMs can be rapidly shared or exported, so you can focus on securing whatever comes next.

Vulnerability Management

Understand the real risk impact. Cybellum analyzes your device software in incredible detail, then matches it with a dedicated product vulnerability database. Clearly understand which vulnerabilities post an immediate threat to your products and which ones less so.

Noise Cancellation - Reduce the noise caused by false positive and low-priority risks with a platform that removes manual vulnerability prioritization.

Industry Focused - Whether in the automotive, medical device, or industrial sector, each field has a unique ecosystem. Gain contextualized insights based on Cybellum's industry specific solutions to better prioritize vulnerabilities and regulatory demands.

Close the loop, from SBOM to Mitigation - Automate SBOM management, VEX generation, and mitigation orchestration, so you get from found to fixed in no time.

Continuous Post Production Assessments - Analyze and mitigate new software updates down the line.

Rapid Compliance with Cybersecurity Regulations - Meet new and existing regulations.

Compliance Management

Automate the entire cyber compliance process. Rapidly identify cyber compliance gaps by matching pre-mapped regulatory requirements with vulnerability assessments, all automatically. Better visibility allows you to generate regulator-ready reports in only a few clicks.

Document - Keep a register of all evidence and relevant regulatory data for historical and auditing purposes, across all product lines and business units.

Stay on top of new standards - Keep up with new and existing regulations, standards and best practices by automatically integrating these policies into your workflow.

Comply faster and get certified - Automated regulatory validation highlights violations and delivers auto-compiled reports, allowing you to see what remains open, then generate detailed reports that perfectly match each standard's structure.

Comply at scale - Ramp up and improve compliance oversight and approval across products and teams.

Easily govern internal policies - Automate internal policy validation using the same engine to make sure all products comply with both internal and external requirements.

Product Incident Response (PSIRT)

Go from detection to investigation under one roof. See your most relevant risks to their post-production products, then facilitate detailed investigations - all in one central location.

Automate PSIRT grunt work so you can focus on thorough investigations - Quickly clear through noise and identify your products' most urgent vulnerabilities. Integrate seamlessly with your SIEM, SOAR, and other operational systems, so you can quickly mitigate incidents.

Keep your finger on the pulse of all security-related events - Take decisive steps against the most relevant cyber risks, all in the context of your specific products and systems. Slash time to remediation and take critical steps towards keeping post-production products continuously secure.

Automate threat intelligence - Automated aggregation and monitoring of threat intelligence sources identify what's relevant to your specific products.

Facilitate entire investigations - Get a workbench for creating and managing investigations, from comprising relevant info, to formulating the analysis, and opening relevant tickets. Then, generate customized reports for each individual stakeholder.

Reduce remediation times - Leveraging pre-existing data about your product's software saves you time on threat monitoring, investigations, and mitigation activities.

Comply faster with post production standards - Ongoing data collection of all product security activities allow you to meet standards from CISA, FDA, IMDRF, ISO, and others.

And Managers can manage it all in one place

Your most pressing issues, ready for action. The most important and impactful insights are waiting for you, allowing you to discover the most widespread vulnerabilities that affect many of your products, uncover the biggest compliance violations faced right now and even identify the riskiest supplier.

See trends over time - Track progress over time, such as the percentage of products at risk, SLA tickets met, average resolution times, and more.

Achieve unprecedented control over your supply chain - See exactly which risks are coming from which supplier or vendor, pinpointing the riskiest components or suppliers.

Gain insights from every angle - Highlight the most crucial security risks, compliance gaps, and licensing challenges at any given moment.

Have full lifecycle visibility - Identify how many products you have at each lifecycle stage, then zero in on their security posture.

Quantify the progress - Put KPIs to product security activities and measure department ROI.

About us

CYBELLUM IS WHERE TEAMS DO PRODUCT SECURITY.

Device manufacturers such as Jaguar Land Rover, Supermicro, Danaher, and Faurecia use Cybellum's Product Security Platform and services to manage cybersecurity risk and compliance across business units and lifecycle stages. From SBOM to Vulnerability Management, Compliance Validation, and Incident Response, teams ensure their connected products are fundamentally secure and compliant – and stay that way.

Experience what product security can be. Book a demo.

Learn more about Product Security

Blogs

The VM Co-Pilot: An Automated Analyst for Product Vulnerability Management

EV Charging Stations: An Emerging Threat for Automotive OEMs

How to Keep the Software Supply Chain Accountable with SBOMs

Podcasts

Knowledge Base

Breaking Down the FDA's 2023 Premarket Cybersecurity Regulations

Learn More →

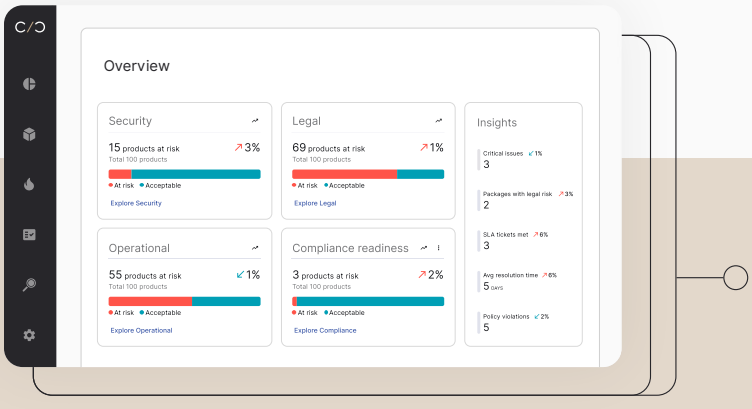
LG Vehicle Component Solutions Case Study

Learn More →

SBOM for Connected Devices: Getting it Right

Learn More →

More about the Product Security Platform



Follow us for news and updates cybellum.com