What US Government Software Suppliers Need to Know about the NIST Secure Software Development Framework

HAMILTON, NJ, USA, July 26, 2022 /EINPresswire.com/ -- The US government has made it clear that it expects its software suppliers to prove they have a secure software development process and that the software they're selling to the government is secure. How exactly that will look at the contract level is yet to be written. But we know where the compliance bar will be set—on the 4 practices and 42 tasks defined in NIST's Secure Software Development Framework (SSDF). If you sell software to the government, you need to know your SSDF "delta" and compliance timeline to maintain a strong competitive position.

> If you sell software within the US government supply chain, now is a great time to leverage this bottom-line oriented podcast to get up to speed on NIST 800-218 and impending regulatory changes."
>
> *John Verry, CISO & Managing Partner, Pivot Point Security*

In the wake of the Solar Winds attacks, President Biden's Executive Order 14028 (specifically Section 4) included a call to action for enhancing security across the government's software supply chain. A direct result of that order is NIST 800-218, "Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities."

What difference does one more NIST "special publication" make? Plenty, if you sell software within the US government supply chain. SSDF compliance is in the process of becoming a mandate for US government agencies and their supply chain partners per changes to Federal Acquisition Regulation (FAR) contract language.

To unpack a wealth of insights into the SSDF and its potential impacts and benefits for SMBs, Elzar Camper, Director of Cyber Security Solutions & Practices at Pivot Point Security, joined the latest episode of The Virtual CISO Podcast. As always, the show's host is John Verry, Pivot Point Security CISO and Managing Partner.

Topics discussed include:

- Why it's so important to take a risk-based approach to implementing security within the software development lifecycle

- The 4 “practices” at the core of secure software development (and the SSDF)
- What a Software Bill of Materials (SBOM) is and isn’t good for
- How the SSDF relates to Executive Order 14028 and other recent US government cyber guidance
- Business benefits of adopting the SSDF, whether you’re mandated to or not

If you sell software anywhere within the US government supply chain, now is a great time to leverage this bottom-line oriented podcast to get up to speed on NIST 800-218 and impending regulatory changes.

The Virtual CISO Podcast by Pivot Point Security

To hear this episode anytime, along with any of the previous episodes in The Virtual CISO Podcast series, visit this page.

About Pivot Point Security
Since 2001, Pivot Point Security has been helping organizations understand and effectively manage their information security risk. We work as a logical extension of your team to simplify the complexities of security and compliance. We’re where to turn—when InfoSec gets challenging.

Richard Rebetti
Pivot Point Security
+1 732-456-5618
email us here
Visit us on social media:
Facebook
LinkedIn