sonatype

An Imminent Need to Secure the Federal Software Supply Chain

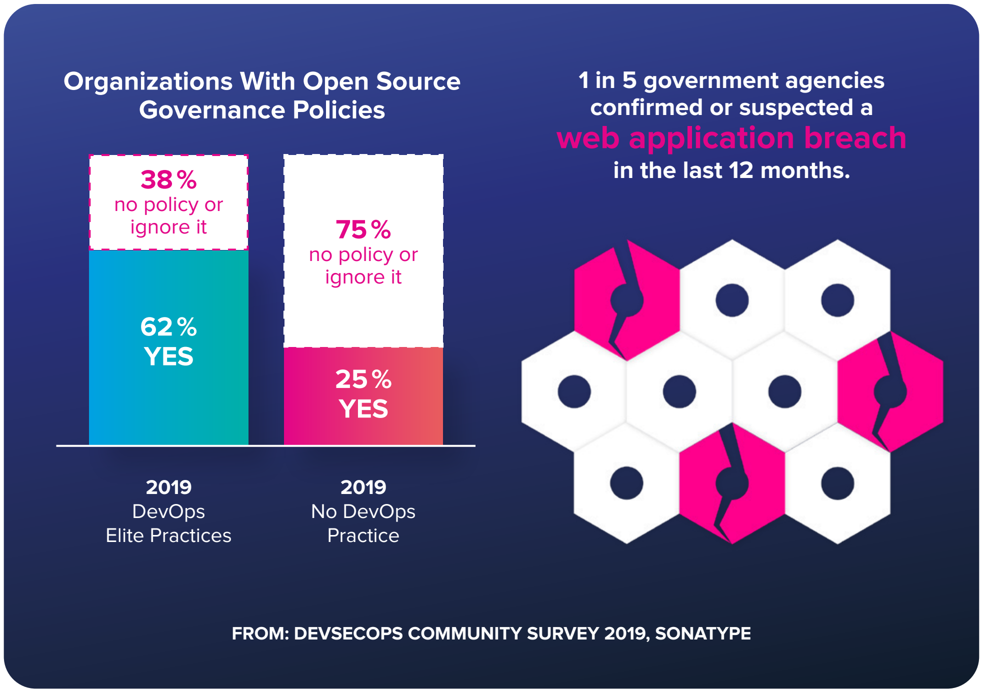
The Security Landscape for the US Government is Changing

The Software Supply Chain

As Marc Andreessen famously observed, “software is eating the world.” The proliferation of software is, indeed, transformational — it is everywhere, in cars, planes, phones, pacemakers, insulin pumps, refrigerators, thermostats, you name it. Nearly all companies are software companies, and that applies to the federal government as well — it may actually be the largest developer of software.

Underpinning all modern technology — software and hardware — is a supply chain. However, even as “software eats the world,” or we could argue “ate the world,” there is still too little understanding of the software supply chain, with continued focus on hardware supply chain. The reality, however, is that software is even easier to pollute than hardware. While there has been an increase in awareness around the need for a coordinated application security strategy, the federal government has historically focused on playing strong defense, putting up walls at the perimeter, at the end of the digital supply chain.

It’s time to shift more security resources further left. In this way, the government can play better offense at the beginning of the digital supply chain so that federal agencies can better protect themselves and the American citizenry.



FROM: DEVSECOPS COMMUNITY SURVEY 2019, SONATYPE

Open Source is Powering Federal Software Development

First, let’s take a step back and understand the current environment. Slowly, agencies are increasingly embracing a concept called DevOps — where the walls between IT operations and developers are torn down, wasteful practices ripped out, and collaboration at scale rewarded.

Enter open source development practices — the miracle drug of choice powering DevOps, and more and more, powering federal software supply chains. These free and readily available open source components allow agencies to save time and money, and in many cases improve quality. This eliminates the reinvention of wheels and exposes software to a global community of “co-developers,” to ideate on and expand upon.

With so many benefits, it’s no wonder that 85% of an application is comprised of open source components. The issue, however, is two-fold. First, not all components are created equal. Sonatype’s research shows that within the Java ecosystem 1 in 10 contains a known security vulnerability, and within Javascript more than 51% of all components have a vulnerability. This highlights the security challenges that agencies are up against.

Second, there is an incredible lack of transparency in how much open source software is being used throughout the federal government. A disconnect between the developers and security teams makes it difficult to rectify this. Open source and DevOps can give the federal government the power to keep up with the commercial industry, but not without proper controls.

The Rise of Regulating Software

We’re in the middle of a paradigm shift in how the federal government develops software and addresses the security issues laid out above.

One of the biggest threats comes from the contractors paid to support the federal government and who are supposed to be helping protect its sophisticated systems. Too often they are inadvertently introducing vulnerabilities into the supply chain. This is due, at least in part, to long-held emphasis on cost and overall performance, rather than security protocols. While the former are important, as cyber security threats multiply daily, the short-term benefit of awarding contracts to the cheapest contractor may have profound long-term effects on national security.

In recent years, however, new legislation and recommendations have begun providing a roadmap for where the U.S. should be headed. There is an opportunity for savvy contractors and agencies to get ahead by prioritizing security in their development process now.

How Can You Keep Up?

As we now know, one of the largest continued areas of mismanagement within the software supply chain continues to be open source components.

The good news — you're not alone, or behind, in tackling this issue. But the time to act is now. Guidance and suggestion will soon turn to regulation and law. As part of this change, all contractors and government software developers will need to think critically and not only ask themselves "does the code have vulnerabilities?" but "*could* it have vulnerabilities?" and "how do we know either way?"

Fortunately, many of the challenges related to the use of known vulnerable software components and software supply chain mismanagement can be easily solved with the right tools. Nicolas Chaillan, chief software officer, U.S. Air Force, and co-lead of the DOD Enterprise DevSecOps Initiative has been particularly vocal about how federal agencies can implement DevSecOps principles and practices into their supply chains.

In explaining the initiative he's co-leading Chaillan noted:

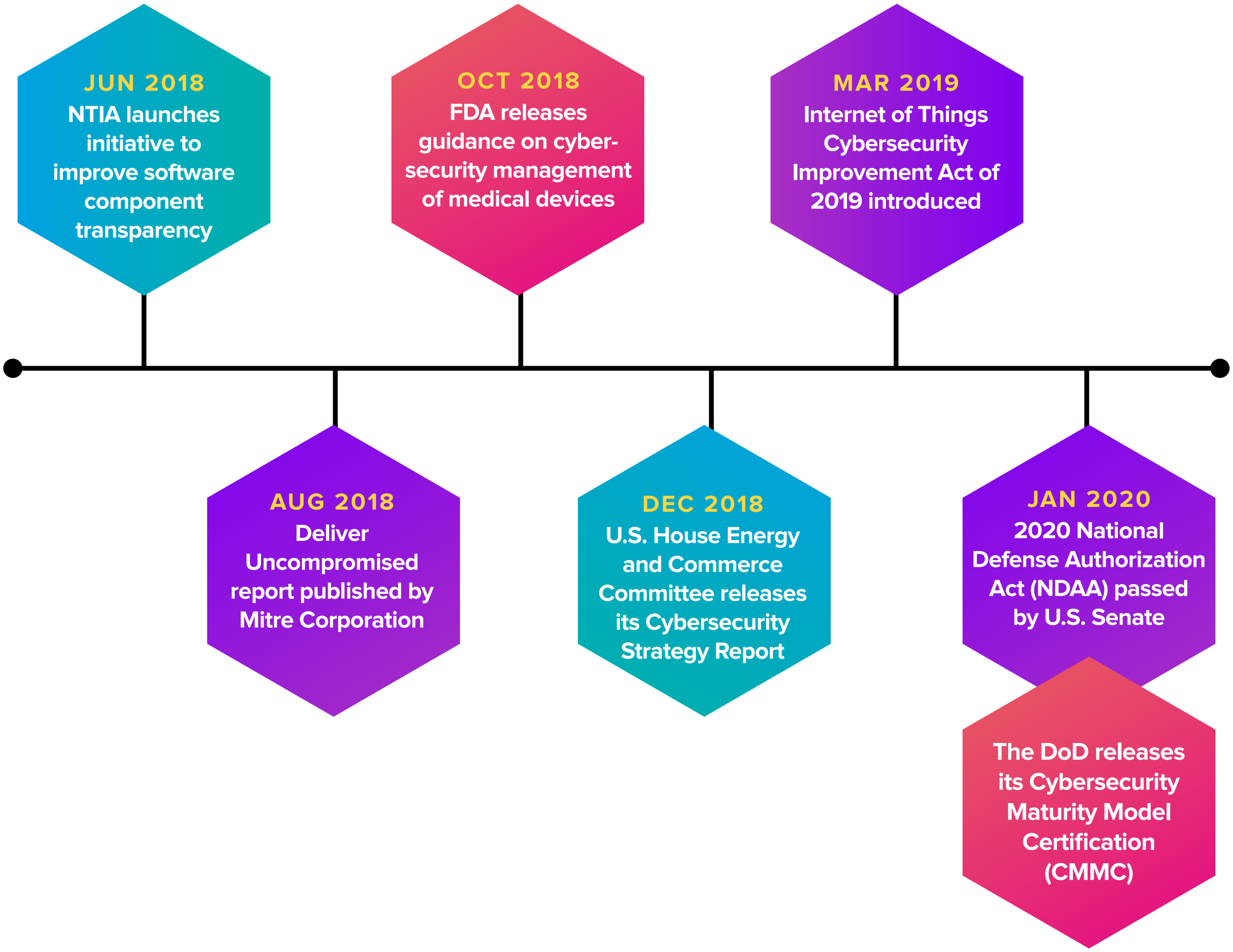
> "The current Department of Defense (DoD) software acquisition process is not responsive to the needs of our warfighters. Therefore, it is difficult for the DoD to keep pace with our potential adversaries and avoid falling behind them. To address this situation, the DoD is pursuing a new software development activity called the DOD Enterprise DevSecOps Initiative. [..] the vision [is] for transforming DoD software acquisition into secure, responsive software factories. It will examine and explore the utilization of modern software development processes and tools to revolutionize the Department's ability to provide responsive, timely, and secure software capabilities for our warfighters.
>
> The focus of the effort involves exploiting automated software tools, services, and standards so warfighters can rapidly create, deploy, and operate software applications in a secure, flexible, and interoperable manner."

We couldn't agree more with Chaillan's mission and believe it's an important step in showing agencies across the country how to implement these types of programs.

For agencies deciding to follow this, automation is imperative. The stark volume of artifacts consumed by organizations today would outpace any attempt to manually review them to determine their health. Machines can accomplish checks in milliseconds where humans might take hours to reach similar conclusions. This reality is akin to the need for robotic analysis of parts being assembled on as high-velocity electronics manufacturing line — human examinations could never keep pace and are prone to error.

The question is not: Can government entities develop secure software? Certainly they can. But changes need to be made now. In today's world, understanding what's in your supply chain is critical to national security.

Regulation Timeline



JUN 2018
NTIA launches initiative to improve software component transparency

AUG 2018
Deliver Uncompromised report published by Mitre Corporation

OCT 2018
FDA releases guidance on cyber-security management of medical devices

DEC 2018
U.S. House Energy and Commerce Committee releases its Cybersecurity Strategy Report

MAR 2019
Internet of Things Cybersecurity Improvement Act of 2019 introduced

JAN 2020
2020 National Defense Authorization Act (NDAA) passed by U.S. Senate

The DoD releases its Cybersecurity Maturity Model Certification (CMMC)

sonatype

Sonatype is the leader in software supply chain automation technology with more than 300 employees, over 1,000 enterprise customers, and is trusted by over 10 million software developers. Sonatype's Nexus platform enables DevOps teams and developers to automatically integrate security at every stage of the modern development pipeline by combining in-depth component intelligence with real-time remediation guidance.

For more information, please visit Sonatype.com, or connect with us on Facebook, Twitter, or LinkedIn.

Headquarters
8161 Maple Lawn Blvd, Suite 250
Fulton, MD 20759
USA • 1.877.866.2836

European Office
199 Bishopsgate
London EC2M 3TY
United Kingdom

APAC Office
5 Martin Place, Level 14
Sydney 2000, NSW
Australia

Sonatype Inc.
www.sonatype.com