

Latest

#SOOCon23: Global Cooperation Needed to Enhance Open Source Software Security

News Topics Features Webinars White Papers Podcasts Events & Conferences Directory

INFOSECURITY MAGAZINE HOME » NEWS » #SOOCON23: GLOBAL COOPERATION NEEDED TO ENHANCE OPEN SOURCE SOFTWARE SECURITY

8 FEB 2023 NEWS

# #SOOCon23: Global Cooperation Needed to Enhance Open Source Software Security



James Coker Deputy Editor, Infosecurity Magazine

[Follow @ReporterCoker](#)

Greater international collaboration is needed in order to strengthen open source software security while retaining its benefits, was the sentiment highlighted by a panel of policymaker experts at the [State of Open Con 23](#) conference, held in London, UK.

Work relating open sources software is already being undertaken by the US Federal government, noted Camille Stewart Gloster, deputy national cyber director, Office for National Cyber Director (ONCD) at the White House. This effort began with [President Joe Biden's zero trust executive order](#) (EO) in May 2021, published in response to the [SolarWinds supply chain attacks](#) in late 2020.

An aspect of this EO was to better understand the products and companies within the federal government's supply chain; for example, requirements for software vendors to provide a Software Bill of Materials (SBOM) as part of their federal procurement process.

*[Join the debate – sign up for Infosecurity Magazine's Online Summit to hear two pros go head-to-head on the validity of SMOBs.](#)*

However, the EO is "just the beginning" of federal government initiatives around open source, commented Stewart Gloster. The White House realises that "software is a key component in our supply chain."

She said the government is now engaging with industry to understand other ways it can support the open source community in strengthening cybersecurity. A notable area the government has identified is driving down the use of memory unsafe languages. Stewart Gloster said that using safe programming language would drive down security vulnerabilities "by up to 70%."

She added that the Biden administration is looking to ensure that the federal government is composed of a variety of skills and backgrounds, including technologists and engineers, to truly

## Related to This Story

[President Biden Has Opened the Door to Zero Trust - Will Boris Johnson Follow Suit?](#)

[LofyGang Group Linked to Recent Software Supply Chain Attacks](#)

[Latest OMB Memo Doubles Down on Flawed NIST Critical Software Standards](#)

[Not Managing Open Source Opens Door for Hackers](#)

understand the effect of policy in areas such as open source.

"At the ONCD we've been very focused on how we evolve towards a digital ecosystem that is secure and resilient," she noted.

Part of this process is "refining the role" the federal government in open source security. Stewart Gloster emphasized that the administration "wants to be informed by the community itself" and that "not everything should be done by government."

Salem Avon, director - Policy, Strategy and Governance Division, United Nations, emphasized the need for synergies and establishing a common purpose globally around the development of open source, similar to efforts taken in areas like human rights and the environment.

It is vital to create "that baseline of things we can come together around," Avon noted.

However, he acknowledged the difficulties around finding consensus around digital issues among the 193 UN member states. Cooperation in this area must begin at the regional level and around specific projects, he said.

"If we can get to that space then I think we can start building up the different tiers that we need in open source in a global way and maybe from that we can start building a larger coalition and consensus," he commented.

He added that among developing nations, the legal frameworks are currently often not in place to ensure technologies like open source software can be used safely and appropriately.

Mike Bracken, founding partner, Public Digital, was keen to point out the enormous benefits and potential offered by open source software, particularly around rapid innovation and creativity. He said there is a danger of governments "rock collecting" around this issue, potentially stifling innovation.

Instead of mimicking types of regulations developed in other areas of technology, there should be an emphasis on how open source can be used positively in delivering public policy, said Bracken.

He added that the use of open source can prevent supply chain software being delivered by a small number of tech vendors.

#RSAC: Open-Source Software is a Public Health Hazard

## What's Hot on Infosecurity Magazine?

Read Shared Watched Editor's Choice

- 6 FEB 2023 NEWS **1** Major Florida Hospital Shuts Down Networks, Ransomware Attack Suspected
- 6 FEB 2023 NEWS **2** Novel Banking Trojan 'PixPirate' Targets Brazil
- 3 FEB 2023 NEWS **3** New Credential-Stealing Campaign By APT34 Targets Middle East Firms
- 18 JAN 2023 NEWS **4** ChatGPT Creates Polymorphic Malware
- 28 JAN 2023 NEWS FEATURE **5** #DataPrivacyWeek: Addressing ChatGPT's Shortfalls in Data Protection Law Compliance
- 14 DEC 2022 BLOG **6** Cybersecurity: Trends From 2022 and Predictions For 2023

### o Comments

 Login ▾

G

LOG IN WITH

OR SIGN UP WITH DISQUS 

Share

**Best** Newest Oldest

Be the first to comment.

[Subscribe](#)

[Privacy](#)

[Do Not Sell My Data](#)

### ALSO ON INFOSECURITY MAGAZINE

2 months ago · 1 comment

**US Sues TikTok Over Child Safety and ...**

2 months ago · 1 comment

**Why the Holidays are the Most ...**

2 months ago

**Securit Found i Million**