Impact of Regulations in the US on the Open Source Software Supply Chain

About Us

- Full service consultancy for managing use of open source software
- Build complete open source management strategies for organizations of all sizes
- Scanning and audit of your codebases to build your SBOMs, and comply with licensing obligations
- Help organizations understand and manage the risks associated with open-source software use
- Provide efficient, comprehensive, and robust implementation of open source programs, and policies

Contents

SBOMs – What Are They?

- Ingredients
- Transparency
- Adoption/ Confusion
- Forecast

Regulation

- In the US:
  - Executive Order 14028 – Improving the Nation's Cybersecurity
  - FDA (US Food and Drug Administration)
  - NHTSA's (National Highway Traffic Safety Administration) 2022 "Cybersecurity Best Practices for the Safety of Modern Vehicles"
- Expectations:
  - Visibility into potential vulnerabilities

OSS CONSULTANTS

Open Source in the Supply Chain

Impact of Regulation

- The automotive industry was one of the earliest adopters of SBOMs
- SBOM’s do not solve cybersecurity challenges
- Best Practices are Still Evolving
- Emerging Trends

Impact of Regulation

- OEM's requirements for specific tooling to generate SBOMs
- SBOM or OSS BoM?
- Lack of regulation for license information
- Formatting differences
- What to do when you receive one?

OSS CONSULTANTS

Impact of Regulation

- Software Defined Vehicles (SDVs) benefit from SBOM's
  - Configuration management
  - Updateability
  - Scalable
  - Better visibility

Takeaways

- Embrace
- Implement
- Focus on Accuracy
- Check your SBOM

OSS CONSULTANTS

OSS CONSULTANTS

Thank You

OSSCONSULTANTS.COM
russ@ossconsultants.com