Secure Software Construction

AUBURN UNIVERSITY

Module 1

Why is Cyber Security Important

AUBURN

2020 — 2021 — 2022 — 2023 →

solarwinds Sunburst

CVE-2021-35211

Kaseya

CVE-2021-30116

Vue.js

CVE-2022-21660

GO ANYWHERE

CVE-2023-0669

LOG4J

CVE-2021-44228

LOG4J

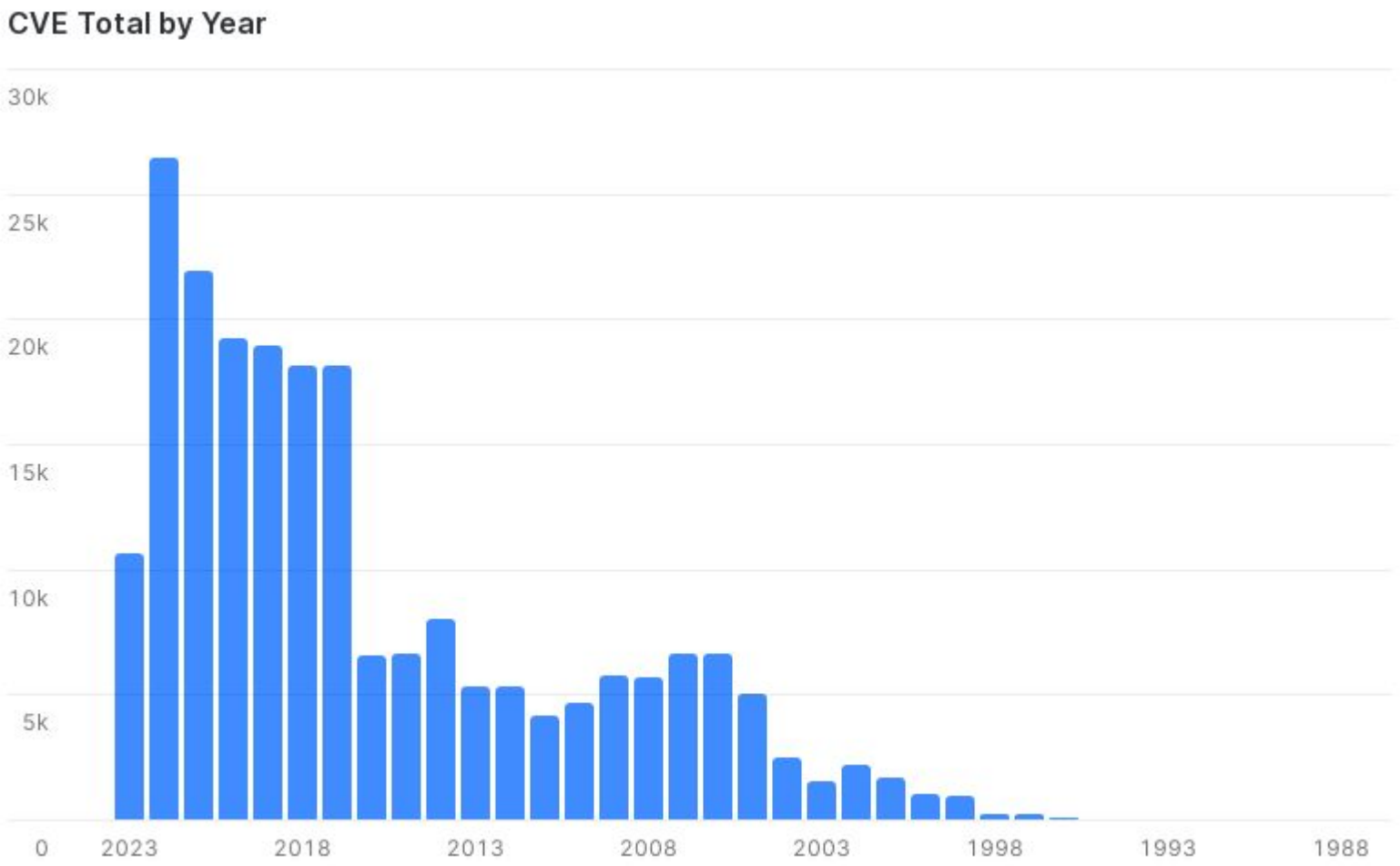
CVE-2021-45046

MoveIt

CVE-2023-34362

CVE Logged By Year

AUBURN

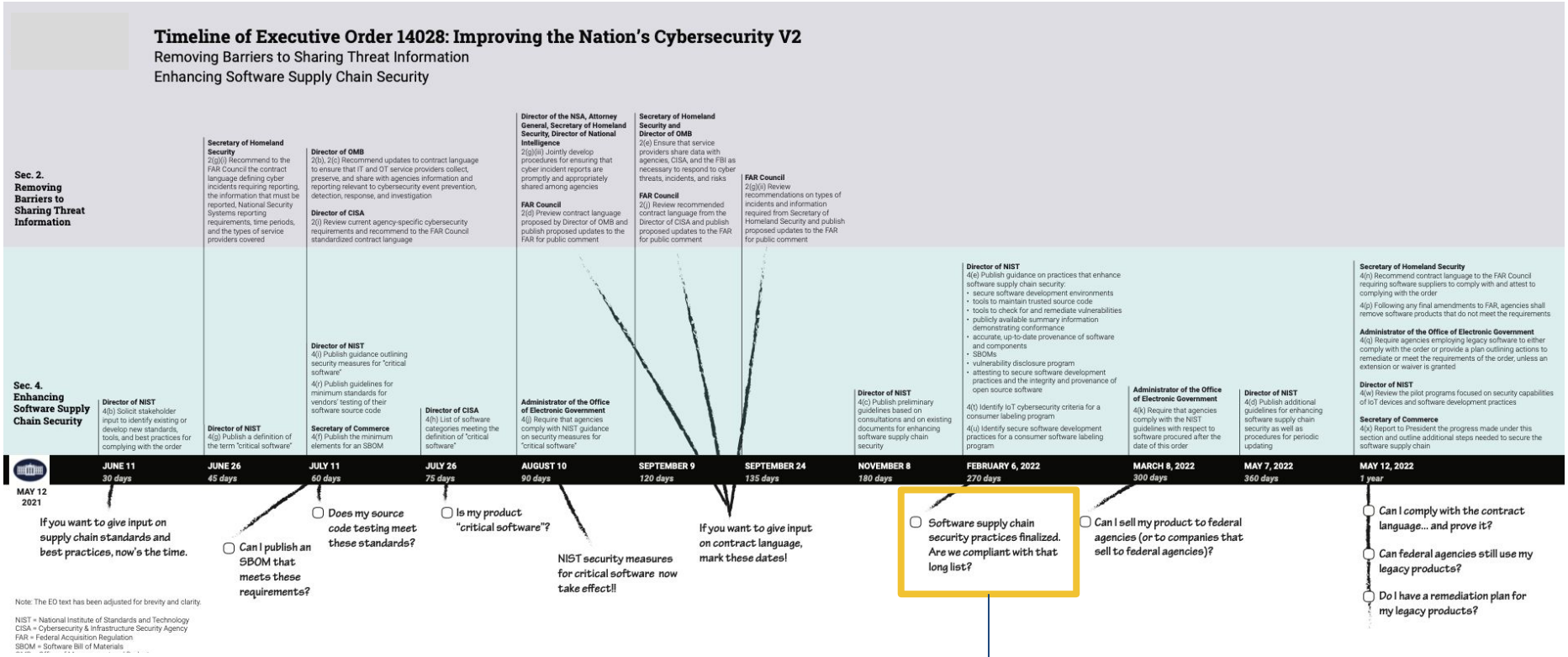


White House Drives Legislation

AUBURN

- Executive Order (EO) 14028 - May 12, 2021
  - "Improving the Nation's Cybersecurity" requiring the government to only purchase software that is developed securely.
  - Sec. 4 - *"Enhancing Software Supply Chain Security"* - **The development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors.** There is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended.
- July 28, 2021 - National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems
- Memorandum M-21-30 - Aug 10, 2021 - Protecting Critical Software Through Enhanced Security Measures
  - Software that controls access to data, cloud-based and hybrid software, software development tools, such as code repository systems, testing software, integration software, packaging software, and deployment software, software components in operational technology (OT).

White House Drives Legislation



Improve Software Supply Chain Security

White House Drives Legislation

AUBURN

Director of NIST

4(e) Publish guidance on practices that enhance software supply chain security:

- secure software development environments
- tools to maintain trusted source code
- tools to check for and remediate vulnerabilities
- publicly available summary information demonstrating conformance
- accurate, up-to-date provenance of software and components
- SBOMs
- vulnerability disclosure program
- attesting to secure software development practices and the integrity and provenance of open source software

4(t) Identify IoT cybersecurity criteria for a consumer labeling program

4(u) Identify secure software development practices for a consumer software labeling program

FEBRUARY 6, 2022

270 days

Improve Software Supply Chain Security

AUBURN

- Establish baseline security standards for development of software sold to the government, including requiring developers to maintain greater visibility into their software and making security data publicly available.
- Establishes concurrent public-private process to develop new and innovative approaches to secure software development and uses the power of Federal procurement to incentivize the market
- Creates a pilot program to create “energy star” type of label so government and public at large can quickly determine whether software was developed securely.
- Focuses on the using the purchasing power of the Federal Government to drive the market to build security into all software from the ground up.

Securing Software Dev Environments

AUBURN

- Separate build environments with administrative controls
- Regular audits of access controls; implement advanced authentication mechanisms (multi factor).
- Employ data encryption
- Employing automated tools with access to trusted source code supply chains, thereby maintaining code integrity
- Automated tools to check for known and potential vulnerabilities to support quick action for remediation or risk mitigation.
- Provide proof of origin of software code or components and controls on internal and 3rd party software components, tools, and services present during development process.
- Perform audits on effectiveness of controls on a recurring basis.
- Software Bill of Materials (SBOM) - what does your software contain?