OpenSSF
OPEN SOURCE SECURITY FOUNDATION

# Key cybersecurity challenges around the globe

## and how the OpenSSF is rising to meet them

# Who is this guy?

CRob, n, adj, and v

Pronunciation: U.S.  (K-rowb)

43rd level Dungeon Master

26th level Securityologist

Pirate-enthusiast & hat-owner

Former Governing Board member and Chairman of the OpenSSF Technical Advisory Council

Chief Security Architect, OpenSSF - Linux Foundation

FIRST PSIRT SIG leader & VulnCon program committee

# What IS the OpenSSF?

- The OpenSSF is a cross-industry collaboration that brings together leaders to improve the security of open source software (OSS) by building a broader community, targeted initiatives, and best practices.

- The OpenSSF brings together open source security initiatives under one foundation to accelerate work through cross-industry support. This is beginning with the Core Infrastructure Initiative and the Open Source Security Coalition, and will include new working groups that address vulnerability disclosures, security tooling and more.

- OpenSSF is committed to collaboration and working both upstream and with existing communities to advance open source security for all.


[What's up with all the Geese?]

# We address 4 key personas within the ecosystem

**OSS Maintainer**

*"I am a developer or maintainer of OSS"*

I *could* also be a STEWARD or MANUFACTURER

**OSS Supplier**

*"I am a commercial company/entity (vendor) that provides a solution or platform that contains OSS to my customers"*

I am a MANUFACTURER

**OSS Consumer**

*"I am a downstream consumer that ingests OSS directly or indirectly"*

I could be a USER, STEWARD, or MANUFACTURER

**CISO + Public Sector**

*"I am a security leader responsible for managing risk at my organization and/or I work within the public sector and am responsible for legislation/regulation that affects OSS"*

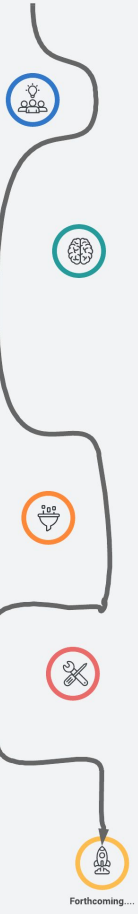
https://github.com/ossf/toolbelt/tree/main/personas

# This is an issue of GLOBAL concern

**Since before computers existed, global governments have been working to protect their citizens**

# Welcome to the awesome World of Global CyberSecurity Compliance

## A Sampling of International CyberSecurity Guideance and Regulations



**Early years ...**

**1914** - USA - Federal Trade Commission Act §5 - an information security regulation and a privacy law.
15 U.S. Code § 45
**1986** - USA - Computer Fraud & Abuse Act - to address the growing threat of computer hacking - HR4718
**1999** - USA - Gramm-Leach-Bliley Act - an information security and a privacy law.
15 U.S. Code Subchapter I

**2000's-2010**

**2000** - ISO/IEC 17799 ->ISO 27002 (renumbered 2007) - guidance and recommendations for information security management systems
**2000** - CA - Personal Information Protection & Electronic Documents Act (PIPEDA) - sets rules for how private-sector organizations collect, use, and disclose personal information in the course of for-profit, commercial activities across Canada
**2002** - USA - Sarbanes-Oxley (SOX) - requires organizations to prove their cybersecurity credentials.
15 US Code Chapter 98
**2002** USA - Homeland Secuirity Act of 2002
**2003** - JP - Act on the Protection of Personal Information (APPI) - Japan's primary data protection legislation,
**2004** - Payment Card Industry Data Security Standard (PCI-DSS) - The payment card industry established this set of security standards to protect cardholder data, a critical piece of sensitive information.
**2004** - US - NIST Cyber Securty Framework (CSF)
**2005** - ISO 27001 - helps organizations manage the security of their information assets. It provides a framework for implementing an information security management system
**2005** - USA - Health Insurance Portability & Accountability Act Privacy Rule (HIPAA) - has security, privacy, and breach notification rules.
45 CFR Part 160, 45 CFR Part 164
**2009** - USA - Health Information Technology for Economic and Clinical Health Act (HITECH) - complements HIPAA by emphasizing electronic health records (EHRs) and the advancement of healthcare information technology.

**2011-2019**

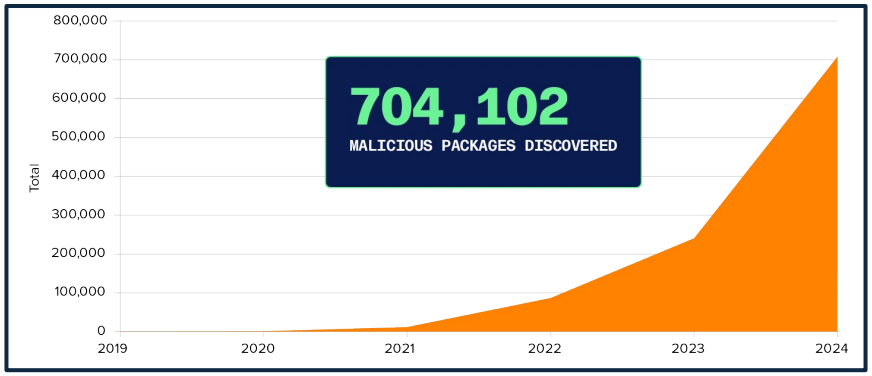
**2011** - USA - NTIA's 1st version of Software Vill of Materials (SBOM) published
**2014** - JP - Basic Cybersecurity Act - first law enacted within the G7 focused on cybersec
**2015** - USA - Cybersecurity Information Sharing Act (CISA) - focuses on improving the communication of cybersecurity threat information between the private sector and the federal government.
**2016** - EU - Directive on Security of Network and Information Systems (NIS) - creates an overall higher level of cybersecurity in the EU
**2016** - EU+USA - EU-US Privacy Shield - framework developed to protect EU residents' data held and processed by organizations in the US - Was invalidated in 2020 with proposed "Trans-Atlantic Data Privacy Framework" being discusssed
**2018** - EU - General Data Protection Regulation (GDPR) - regulates how personal data of individuals within the EU can be collected, processed, and transferred.
Corrigendum to Regulation (EU) 2016/679
**2019** - USA - NIST Secure Software Development Framework (SSDF) - NIST SP 800-218

**"Modern" Guidance**

**2021** - USA - WH Executive Order 14028: Improving the Nations Cybersecurity - equires US agencies to enhance cybersecurity and software supply chain integrity.
**2021** - USA - CISA's SBOM Minimum elements published
**2022** - JP - Revision of National Security Strategy (NSS), National Defense Strategy (NDS), and Defense Buildup Program (DBP) - Updates to improve the response capabilities [of Japan] in the field of cybersecurity
**2022** - EU - Digital Operationl Resilience Act (DORA) - to improve the digital operational resilience of financial entities in the EU and their ICT suppliers and create a uniform regulatory framework across the EU
**2023** - EU - NIS2 - aims to extend the scope of obligations on entities required to take measures to increase their cybersecurity capabilities.
**2023** - JP - METI - Guide of Introduction of Software Bill of Materials (SBOM) for Software Management -
**2023** - IN - Digital Personal Data Protection Act - India's first comprehensive data protection law, designed to protect the privacy of individuals
**2024** - EU- Cyber Resilience Act (CRA) - an EU-wide cybersecurity certification framework for digital products, services and processes. It complements the NIS Directive

**Forthcoming....**

# A Tour of many “popular” open source & supply chain attacks over the years




<- The “OG” Supply Chain attack 1194–1184 BC

<- Typically the 1st time “supply chain attack” was recognized as an issue in cybersec

1/1/2010 1/1/2011 1/1/2012 1/1/2013 1/1/2014 1/1/2015 1/1/2016 1/1/2017 1/1/2018 1/1/2019 1/1/2020 1/1/2021 1/1/2022 1/1/2023 1/1/2024 12/31/2024

https://www.sonatype.com/resources/vulnerability-timeline
https://www.reversinglabs.com/blog/a-partial-history-of-software-supply-chain-attacks
https://linuxfoundation.eu/newsroom/the-rising-threat-of-software-supply-chain-attacks-managing-dependencies-of-open-source-projects

# Key EU Legislation

**2016** - EU - Directive on Security of Network and Information Systems (NIS) - creates an overall higher level of cybersecurity in the EU

**2016** - EU+USA - EU-US Privacy Shield - framework developed to protect EU residents' data held and processed by organizations in the US. - Was invalidated 2020 with proposed "Trans-Atlantic Data Privacy Framework" being discussed

**2018** - EU - General Data Protection Regulation (GDPR) - regulates how personal of individuals within the EU can be collected, processed, and transferred. Regulation (EU) 2016/679

**2022** - EU - Digital Operational Resilience Act (DORA) - to improve the digital operational resilience of financial entities in the EU and their ICT suppliers and create a uniform regulatory framework across the EU

**2022** - EU - NIS2 - aims to extend the scope of obligations on entities required to take measures to increase their cybersecurity capabilities.

**2024** - EU AI Act - ensures that AI systems are trustworthy and respect fundamental rights, safety, and ethical principles. (Globally the 1st law around AI-regulation)

**2024** - EU- Cyber Resilience Act (CRA) - an EU-wide cybersecurity certification framework for digital products, services and processes. It complements the NIS Directive

# ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004

Has a library of best practices, implementation guides, member guidance, and other cybersecurity artifacts including:


13 JUNE, 2023

**Good Practices for Supply Chain Cybersecurity**

The report provides an overview of the current supply chain cybersecurity practices followed by essential and important entities in the EU, based on the results of a 2022 ENISA study which focused on investments of cybersecurity budgets among...

Cybersecurity of Critical Sectors | State of cybersecurity in the EU | National Cybersecurity Strategies | National / EU authorities | Private Sector

# German Federal Office for Information Security (BSI)

Protecting government networks and securing core network gateways, develops binding security standards for government agencies in relation to IT procurement and deployment. The BSI is the Central Reporting Office for IT Security within the German federal administration.

BSI TR-03183: Cyber Resilience Requirements for Manufacturers and Products

Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products - Part 1: General requirements Version 0.9.0

date 10.10.2024

Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products - Part 2: Software Bill of Materials (SBOM) Version 2.0.0

date 10.10.2024

Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products - Part 3: Vulnerability Reports and Notifications

date 10.10.2024

# Key US Legislation


**1986 -** USA - Computer Fraud & Abuse Act - to address the growing threat of computer hacking - HR4718
**1999** - USA - Gramm-Leach-Billey Act - an information security and a privacy law.
15 U.S. Code Subchapter I
**2002** - USA - Sarbanes-Oxley (SOX) - requires organizations to prove their cybersecurity credentials.
15 US Code Chapter 98
**2002** - USA - Homeland Security Act of 2002
**2005** - USA - Health Insurance Portability & Accountability Act Privacy Rule (HIPAA) - has security, privacy, and breach notification rules.
45 CFR Part 160, 45 CFR Part 164
**2009** - USA - Health Information Technology for Economic and Clinical Health Act (HITECH) - complements HIPAA by emphasizing electronic health records (EHRs) and the advancement of healthcare information technology.

# Other US “Greatest Hits”

(these are NOT laws)

**2004 -** Payment Card Industry Data Security Standard (PCI-DSS) - The payment card industry established this set of security standards to protect cardholder data, a critical piece of sensitive information.
**2004** - USA - NIST Cyber Security Framework (CSF)
**2011** - USA - NTIA's 1st version of Software Bill of Materials (SBOM) published
**2019** - USA - NIST Secure Software Development Framework (SSDF) - NIST SP 800-218
**2021** - USA - WH Executive Order 14028: Improving the Nation's Cybersecurity - equires US agencies to enhance cybersecurity and software supply chain integrity.
**2021** - USA - CISA's SBOM Minimum elements published

# The National Institute of Standards and Technology (NIST)

Advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

NIST Special Publication 800-53
Revision 5

**Security and Privacy Controls for Information Systems and Organizations**

The NIST Cybersecurity Framework (CSF) 2.0

NIST Special Publication 800-218

**Secure Software Development Framework (SSDF) Version 1.1:**

*Recommendations for Mitigating the Risk of Software Vulnerabilities*

# Cybersecurity and Infrastructure Security Agency (CISA)

Lead the national effort to understand, manage, and reduce risk to US cyber and physical infrastructure.



Types of Software Bill of Material (SBOM) Documents

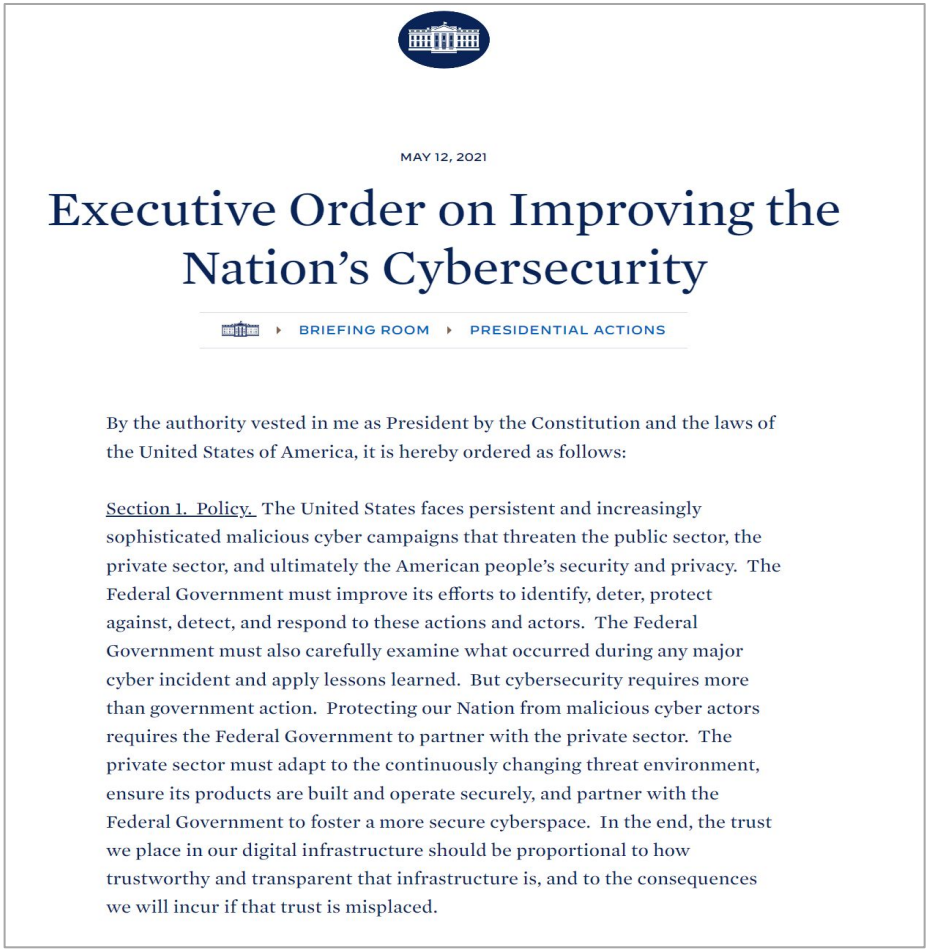
Minimum Requirements for Vulnerability Exploitability eXchange (VEX)

**CISA Open Source Software Security Roadmap**

# WH EO 14028

In May of 2021 and followed-up in January of 2022, the U.S. White House issued guidance for improving cybersecurity.

It speaks **directly** to software supply chain, software bill of materials, and secure software development practices



MAY 12, 2021

## Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM ▸ PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

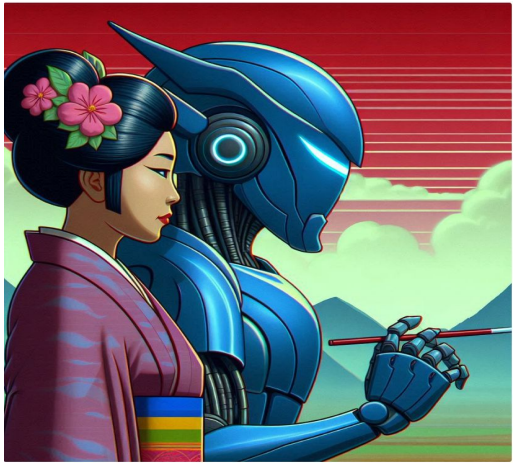
Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Want to learn more?

https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

# Japan Legislation & Guidance



**2003** - JP - Act on the Protection of Personal Information (APPI) - Japan's primary data protection legislation,
**2014** - JP - Basic Cybersecurity Act - first law enacted within the G7 focused on cybersec
**2022** - JP - Revision of National Security Strategy (NSS), National Defense Strategy (NDS), and Defense Buildup Program (DBP) - . Updates to improve the response capabilities [of Japan] in the field of cybersecurity
**2023** - METI - "Guide of Introduction of Software Bill of Materials (SBOM) for Software Management" - https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html

# Australia Legislation

**2018** - Security of Critical Infrastructure Act 2018 (SOCI Act)

**2024** - Cyber Security Act - Australia's 1st stand-alone cyber law

# Canada Legislation

**2000 –** CA - Personal Information Protection & Electronic Documents Act (PIPEDA) - sets rules for how private-sector organizations collect, use, and disclose personal information in the course of for-profit, commercial activities across Canada

**2022** - CA - Bill C-26, also known as the An Act Respecting Cyber Security (ARCS) - provided new cybersecurity protections for telecommunications service providers in Canada as well as to ensure that they take certain measures to mitigate or remedy cybersecurity risks.

**PENDING** - Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and related amendments to other Acts (Digital Charter Implementation Act, 2022), was introduced to overhaul PIPEDA and modernize the framework for the protection of personal information in the private sector.

# People's Republic of China Legislation

**2006** - Public Security Administration Punishments Law - addresses the consequences of invading a computer information system.

**2016** - Cybersecurity Law (CSL) - The first cybersecurity law in China. The CSL regulates the construction, operation, and maintenance of networks in China. It also establishes frameworks for protecting critical information infrastructure and the Multi-Level Protection Scheme.

**2020** - Personal Information Protection National Standard - Requires data controllers to implement measures to manage third-party products and services that collect personal information.

**2021** - Data Security Law (DSL) - Focused on protecting data security from a national security perspective. The DSL classifies data based on its potential impact on national security and regulates how it is stored and transferred.

**2021** - Personal Information Protection Law (PIPL) - PIPL is China's comprehensive privacy law. It is considered to be comparable to other major global data privacy laws, such as the European Union's General Data Protection Regulation (GDPR).

# India Legislation

**2000** - The Information Technology Act - India's 1st cyber security legislation

**2011** - Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules

**2013** - National Cyber Security Policy

**2021** - Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules - Replaces 2011 IT Rules

**2023** - Digital Personal Data Protection Act (DPDP)

# United Kingdom Legislation


**1990** - Computer Misuse Act - the main cybersecurity act that regulates the UK's digital relationship between individuals and malicious parties.

**2018** - Data Protection Act (DPA) - primary law on personal data processing in the UK, which is enforced along with the UK-GDPR

**2021 -** UK-GDPR (General Data Protection Regulation) is the United Kingdom's data security regulation, tailored by and complementing the Data Protection Act 2018. Also modeled after the EU-GDPR, it governs and regulates how UK organizations and businesses collect, store, use, and process personal data.

**2021** - Telecommunications (Security) Act - The Telecommunications (Security) Act, which came into effect in November 2021 (full implementation expected by March 2024), is a strict, all-encompassing act that regulates the network security against cyberattacks of all mobile carriers in the UK.

**2022 -** UK Operational Resilience Framework - a regulatory initiative developed by the Bank of England, the Prudential Regulation Authority (PRA), and the Financial Conduct Authority (FCA) to ensure that financial institutions and other regulated firms can withstand and recover from operational disruptions.

# Collectively, these mandate things like…


- Transparency & Reporting cybersecurity incidents & vulnerabilities
- Produce Software Bill of Materials (SBOM)
- Evaluate security practices of developers and within supply chains
- Suppliers must look for and remediate known vulnerabilities
- Education and standards around cyber and development security

# What's Up With That?

Image Source

**SBOM - Software Bill of Materials -** an electronic manifest of all the components in a given piece of software
**SDLC - Software Development Lifecycle -** mature, phased process for developing software
**CVD - Coordinated Vulnerability Disclosure -** Practice of disclosing security bugs to affected parties in a managed manner
**VEX - Vulnerability EXchange -** security advisory format that allows maintainers to express the affectedness of their software to a security issue

# OpenSSF initiatives that support these efforts

# Working Groups, Projects, & SIGs

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

## 1. INFORM

### Vulnerability Disclosures
*Efficient vulnerability reporting and remediation*

I. **CVD Guides** SIGs
J. **OSS-SIRT** SIG
K. **Open Source Vuln Schema (OSV)** project
L. **OpenVEX** project
**OpenVEX** SIG
M. **Vuln Autofix** SIG
Table Top Exercises - TTX

### Metrics & Metadata
*Security metrics/reviews for open source projects*

N. **Security Insights** project
O. **Metrics API** SIG
P. **Security Reviews** project

### Securing Critical Projects
*Identification of critical open source projects*

U. **List of Critical OS Prj. components, & Frameworks** SIG
V. **criticality_score** project
W. **Census** SIG
X. **Package Analysis** project
Y. **allstar** project

## 2. EQUIP

### Best Practices
*Identification, awareness, and education of security best practices*

A. **Secure Software Development Fundamentals courses** SIG
B. **Security Knowledge Framework (SKF)** project
C. **OpenSSF Best Practices Badge** project
D. **OpenSSF Scorecard** project
E. **Common Requirements Enumeration (CRE)** project
F. **Concise & Best Practices Guides** SIGs
G. **Education** SIG
H. **Memory Safety** SIG
AG. **The Security Toolbelt** SIG
AL. Python Hardening SIG

### Security Tooling
*State of the art security tools*

Q. **SBOM Everywhere** SIG
R. **OSS Fuzzing** project
AI. **SBOMit** project
AJ. **Protobom** project

### AI/ML Security
*AI/ML Security at the Intersection of Artificial Intelligence and Cybersecurity*

AD. **Model Signing** SIG

### Supply Chain Integrity
*Ensuring the provenance of open source code*

S. **Supply-chain Levels for Software Artifacts (SLSA)** project
T. **Secure Supply Chain Consumpt Framework (S2C2F)** project
AJ. **gittuf** project
AK. **GUAC** project
AM. **Zarf** project

### DevRel
*Develop Use Cases and help others learn about security*

### Diversity, Equity, & Inclusion
*Increase representation and strengthen the overall effectiveness of the cybersecurity workforce*

## 3. ENGAGE

### End Users
*Voice of public & private sector orgs that primarily consume open source*

Z. **Threat Modeling** SIG

### Securing Software Repositories
*collaboration between repository operators*

AB. **RSTUF** Project

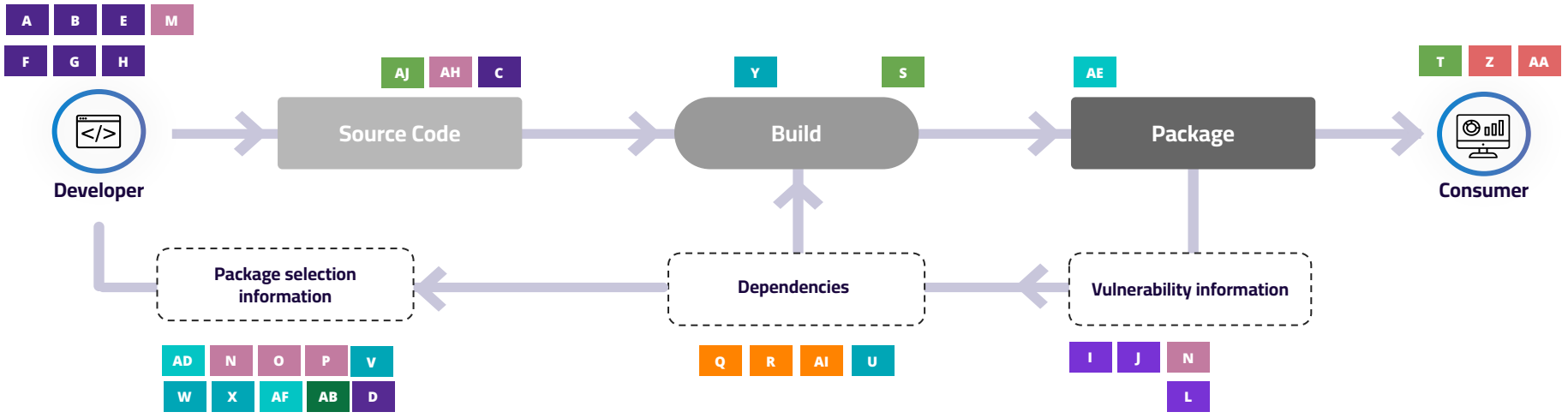
### Projects
*Category-leading software initiatives*

AE. **Sigstore**
AF. Core Toolchain Infrastructure (CTI)

https://openssf.org/community/openssf-working-groups

https://openssf.org/projects/

# How OpenSSF Projects & SIGs Work Together ("CI/CD View")




## Best Practices

A. Secure Software Development Fundamentals courses SIG
B. Security Knowledge Framework (SKF) project
C. OpenSSF Best Practices Badge project
D. OpenSSF Scorecard project
E. Common Requirements Enumeration (CRE) project
F. Concise & Best Practices Guides SIGs
G. Education SIG
H. Memory Safety SIG

## DevRel Community

## Vulnerability Disclosures

I. CVD Guides SIGs
J. OSS-SIRT SIG
K. Open Source Vuln Schema (OSV) project
L. OpenVEX SIG
M. Vuln Autofix SIG

## Metrics & Metadata

N. Security Insights
O. Security-Metrics: Risk Dashboard project
P. Security Reviews project
AH. Security Insights Spec project

## Security Tooling

Q. SBOM Everywhere SIG
R. OSS Fuzzing SIG
AI. SBOMit project
AJ. Protobom project

## Supply Chain Integrity

S. SLSA project
T. S2C2F project
AJ. Gittuf project
AK. GUAC project

## Securing Critical Projects

U. List of Critical OS Projects SIG
V. criticality_score project
W. Harvard study SIG
X. Package Analysis project
Y. allstar project

## End Users

Z. Threat Modeling SIG

## Securing Software Repositories

AB. Repository as a Service Project

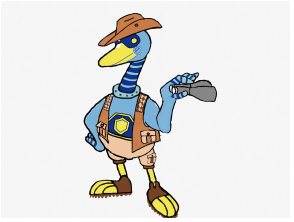
## AI/ML Security

## Diversity, Equity, & Inclusion

## Projects

AD. Alpha & Omega project
AE. Sigstore
AF. Core Toolchain Infrastructure (CTI)

# Vulnerability Disclosure



Vulnerability Handling/Coordinated Vulnerability Disclosure is mentioned on 30 of the 81 pages of the legislation and annexes.

The OpenSSF has a Vulnerability Disclosures working group that focuses on this part of the ecosystem.

## Cvd guides + policy templates

- Coordinated Disclosure Guides for OSS Maintainers/Projects, Security Researchers, and OSS Consumers (forthcoming)
- Security Policy templates

## Table Top Exercises (TTX)

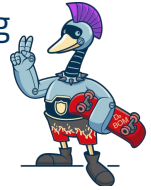
- TTX Framework
- Historic TTX exercises
- Delivering Mock Incidents at events

## SIREN Threat Mailing List

- Community mailing list to share known and actively exploited vulnerabilities
- Support for the oss-security and distros mailing lists

## OpenVEX Schema + tooling

- Simple data format and tooling to issue VEX statements to manage affectedness information about vulns



## OSV Schema + tooling

- Vuln metadata schema that powers the OSS OSV vuln database & tooling.
- Broadly used by upstream distros and community to catalog vulnerabilities & enrich data

## Coming soon! Advise (formerly known as VINCE)

- Open source CVD platform/software

# Dropping the BOM

CycloneDX

SPDX

*r(77) -*

*“In order to facilitate vulnerability analysis, manufacturers should identify and document components contained in the products with digital elements, including by drawing up an SBOM. An SBOM can provide those who manufacture, purchase, and operate software with information that enhances their understanding of the supply chain, which has multiple benefits, in particular it helps manufacturers and users to track known newly emerged vulnerabilities and cybersecurity risks. It is of particular importance that manufacturers ensure that their products with digital elements do not contain vulnerable components developed by third parties. Manufacturers should not be obliged to make the SBOM public.”*

## Protobom

A protocol buffers representation of SBOM data able to ingest documents in modern SPDX and CycloneDX versions without loss.

## bomctl

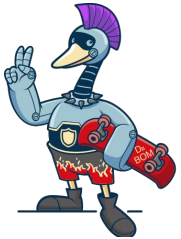
format-agnostic SBOM tooling, which is intended to bridge the gap between SBOM generation and SBOM analysis tools.

## GUAC

Fills in the gaps by ingesting software metadata, like SBOMs, and mapping out relationships between software.

## SBOMit

An SBOM format-independent method for attesting components with additional verification information.



## OpenVEX

A simplified implementation of VEX vulnerability affectedness

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

# Putting things together

# Gooseatron9000 Uber-patterns – "The Security Toolbelt"

"Producer"

"The Software Factory"

"Consumer"

CAPABILITIES

Secure Developer

Secure Dev Env.

Secure SCM

Secure Build/ CI

Secure Publication / Distribution

Secure Ingestion

Secure Implementation

Secure Maintenance

Cross-Cutting Capabilities

Supply Chain Metadata Storage

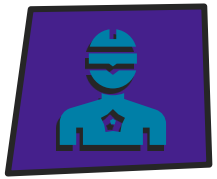
Supply Chain Control Plane

# Enter the Open Source Project Security (OSPS) Baseline

<insert dramatic music>

Some of you may know these as “IT Grundschutz”

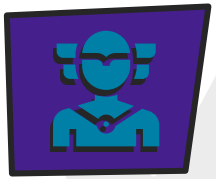
# What is a baseline, and why does it matter to me?



## Definition

Often seen in enterprise operations, a Baseline is defined by NIST SP 800-37 Rev. 2 as

"The set of controls that are applicable to information or an information system to meet legal, regulatory, or policy requirements, as well as address protection needs for the purpose of managing risk."



## TL/dr

"A set of security requirements that help an organization or project meet specific security objectives".

# Standards + frameworks-based criteria

## ACCESS CONTROL

How is access and changes to the code and pipeline managed?

## DOCUMENTATION

What does the project state about how they manage the code and react to vulnerability reports?

## LEGAL

What licenses are in place for the project?

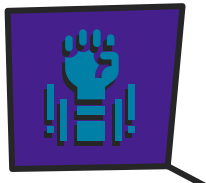
## BUILD + RELEASE

How are the CI/CD pipelines configured and managed?

## QUALITY

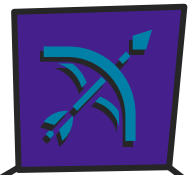
What testing and change management are in place?

# Global Frameworks



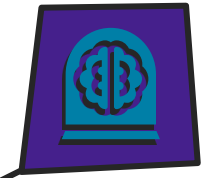
## ISO 27001
## ISO 27002

International InfoSec frameworks



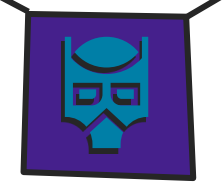
## EU CRA

The Cyber Resilience Act



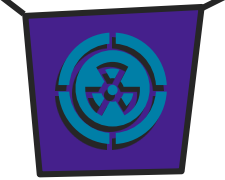
## NIST SSDF 1.1

NIST's Secure Software Development Framework



## CSA CCM V4

Cloud Security Alliance's Cloud Controls Matrix



## NIST CSF 2.0

NIST's Cyber Security Framework

## ...AND MANY OTHERS!

# Compliance Crosswalk (future deliverable)

| WIP - Best Practices: Future | | | | | | | OpenSSF Mappings | | | CRA+ PLD | SSDF 1.1 | NIST CSFv2 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Use present tense**: State what is actively enforced or applied now. Allows for T/F result.<br>**Start with the item that should be evaluated**: Begin each statement with the subject (e.g., "Permissions" or "All software releases").<br>**Actionable verbs**: Use clear, action-oriented verbs like "require," "restrict," "ensure."<br>**Name a specific control activity**: Include relevant details to clarify the action being taken.<br>**Consistent terminology**: Use terms uniformly to avoid ambiguity.<br>Example Format:<br>Subject + Action + Control Activity (e.g., "Permissions are scoped to reduce access to only those necessary for performing operations.") | | | **Explain the purpose**: Describe why the check is valuable or necessary.<br>**Highlight risk mitigation**: Identify the risks addressed by the check.<br>**Reference standards**: Mention relevant regulations or industry best practices.<br>**Discuss consequences**: Explain what could happen if the check isn't followed.<br>**Be concise**: Keep the explanation clear and to the point.<br>**Emphasize prevention**: Focus on how the check prevents issues. | | **Level 1** should contain criteria that would benefit any code or non-code project with any number of maintainers or users. (this definition is WIP)<br>**Level 2** should contain criteria that would benefit any code project that has at least 2 maintainers and a small number of consistent users. (this definition is WIP)<br>**Level 3** should contain criteria for any code project that has a large number of consistent users. | **BP Badges Text** | **Scorecard Probe** | **Security Insights Value** | This column has all of the CRA, CRA Annex, and PLD requirements | This column has the NIST SSDF (800-218) requirements | This column has the NIST Cyber Security Framework v2 requirements |
| **Category** | **Criteria ID** | **Revised Criteria Statement** | **Maturity Level** | **Notes** | **OSPS Suggestions** | | **this column has all of the "passing" BP criteria** | | | | | |
| Access Control | OSPS-AC-01 | The project's **version control system** MUST require multi-factor authentication (MFA) for users when modifying the project repositories or accessing sensitive data. | 1 (sandbox) | Multi-factor authentication (MFA) significantly reduces the risk of unauthorized access by adding an extra layer of security beyond passwords. By requiring MFA for modifications to project repositories or access to sensitive data, the organization mitigates the threat of credential theft and ensures compliance with security best practices and industry standards. This proactive approach helps prevent security breaches and protects critical assets. | MFA is enforced for modifications across the VCS organization where the project is hosted | | The project MUST require two-factor authentication (2FA) for developers for changing a central repository or accessing sensitive data (such as private vulnerability reports). This 2FA mechanism MAY use mechanisms without cryptographic mechanisms such as SMS, though that is not recommended.<br>The project MUST require two-factor authentication (2FA) for developers for changing a central repository or accessing sensitive data (such as private vulnerability reports). | | | 1.2d, 1.2e, 1.2f | PO3.2, PS1 | PR.AA-02 |
| Access Control | OSPS-AC-02 | The project's **version control system** MUST restrict collaborator permissions to the lowest available privileges by default. | 1 (sandbox) | Restricting default member permissions to the lowest available level for the version control system helps minimize the risk of unauthorized or accidental changes by limiting access to only essential actions. This principle of least privilege ensures that users have only the permissions necessary for their role, reducing the attack surface and the potential impact of compromised accounts. It also aligns with security best practices by preventing unnecessary privilege escalation. | Default member permissions are restricted in the VCS organization where the project is hosted | | | | | 1.2f | PO2, PO3.2, PS1 | PR.AA-02 |
| Access Control | OSPS-AC-03 | The project's version control system MUST prevent unintentional direct commits against the primary branch. | 1 (sandbox) | Preventing accidental direct commits to the default branch helps maintain the stability and integrity of the codebase. By enforcing this control, only thoroughly reviewed and tested code can be merged, reducing the risk of introducing unapproved or faulty changes. This aligns with best practices for version control and ensures that critical branches are protected from unintended modifications. | Direct commits are automatically prevented on the default VCS branch | | | Branch-Protection | | 1.2f | PO3.2, PS1 | PR.AA-02 |
| Access Control | OSPS-AC-04 | The project's version control system MUST prevent unintentional deletion of the primary branch. | 1 (sandbox) | Preventing accidental deletion of the default branch safeguards the core of the project, ensuring that critical code is not lost or disrupted. This control mitigates the risk of significant data loss or project downtime and aligns with best practices for protecting essential assets in version control systems. | Deletion is automatically prevented on the default VCS branch | | | Branch-Protection | | 1.2b, 1.2f | PO3.2, PS1 | PR.AA-02 |

DRAFT - https://docs.google.com/spreadsheets/d/1an5mx3rayoz3JRFUepD56zgprpwXBXBG70fVZvIMCpA/edit?gid=1198757870

# Bringing together your favourite ossf tools!

## Best Practices Badges


Interview-based verification of security practices

## Scorecard


Automated checking of 19 security aspects of a project

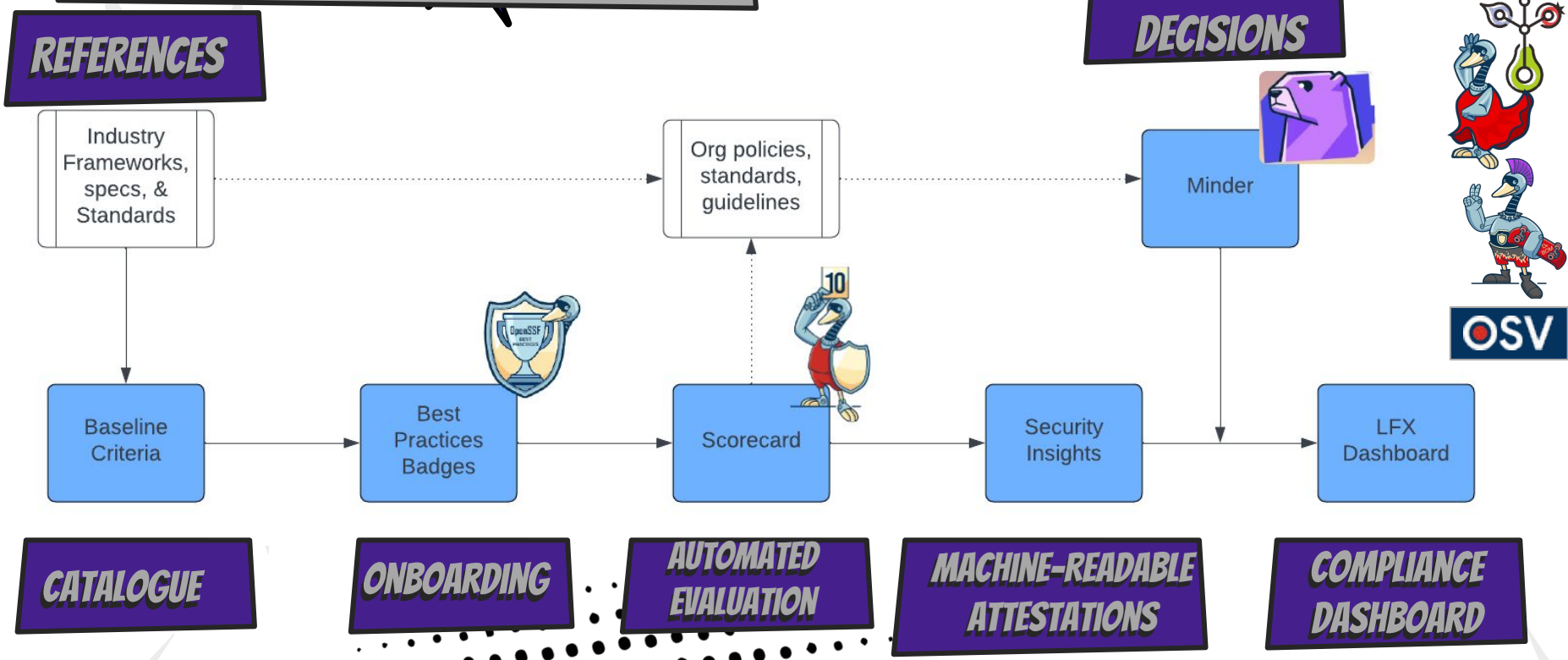
## Security Insights

Machine-readable output of assertions

## MINDER

Policy-driven decisions on desired security criteria

# Future Workflow




CycloneDX

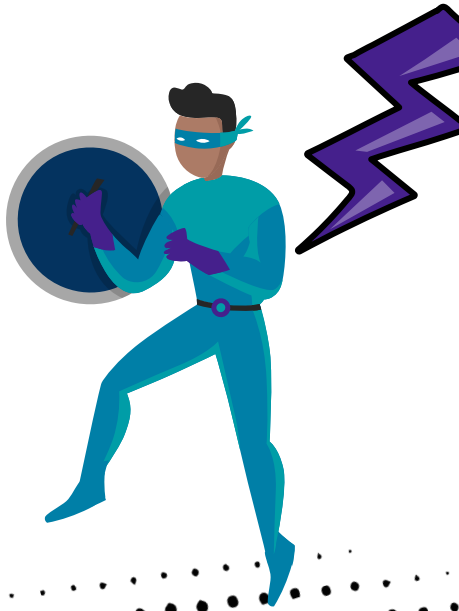
SPDX

OSV

# Baseline Roadmap

## NOW

- Work with 6 Pilot OSSF projects to implement the Baseline
- Work with 3 CNCF or FINOS projects to implement the Baseline
- Complete Compliance Crosswalk & publish
- Complete process documentation for updating & rolling out new/revised Baseline criteria



## NEXT

- 2025 - Complete integration with Best Practices Badge, Scorecard, Insights, Minder, & LFX
- 2025 - Work with broader LF on Baseline adoption
- 2025 - All OpenSSF projects aligned to Baseline
- 2025 - Develop automation for high-priority tasks to achieve Baseline compliance

The BEST way to help make open source better is to PARTICIPATE!

# Get involved!

- Many other OpenSSF projects/SIGs, some in early stages
  - Supply chain Levels for Software Artifacts (SLSA) slsa.dev
  - “SBOM Everywhere” tool work
  - Education work (deeper, K-12, manager, etc.)
  - Metrics Dashboard SIG—easily see status of an OSS project
  - OSS critical projects identification
  - Secure Supply Chain Consumption Framework (S2C2F) (was SSC)
- To get involved in OpenSSF see openssf.org
  - Biweekly meetings, mailing lists, Slack
  - See our blog for what’s going on: openssf.org/blog
- Many other OSS projects & foundations, e.g., Continuous Delivery
- Industry, academia, & government should work together
- The best way to influence an OSS project direction is to get involved!

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

# Thanks!

@~~SecurityCRob~~

@SecurityCRob@infosec.exchange

https://github.com/SecurityCRob

The Security Unhappy Hour,
Chips & Salsa
What's in the SOSS?

https://www.linkedin.com/in/darthcrob/

# This presentation is released under the CC-BY-4.0 license


# Supplemental Materials

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

# OpenSSF Technical Initiatives

# Course—Developing Secure Software (LFD121)

*Free* course, 14-18 hours, with 3 parts:

- Requirements, Design, and Reuse
- Implementation
- Verification and More Specialized Topics

Teaches fundamentals of developing **any** secure software (**OSS or not**)


Free certificate of completion when you take LFD121
https://training.linuxfoundation.org/training/developing-secure-software-lfd121

OSS Maintainer

OSS Consumer

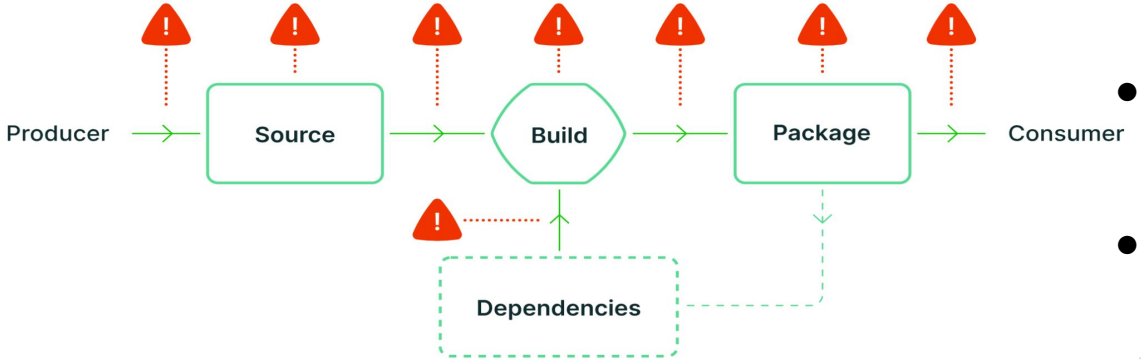
# OpenSSF Best Practices Badge


- Identifies best practices for OSS projects
  - Goal: Increase likelihood of better quality & security. E.g.:
    - "The project sites… MUST support HTTPS using TLS."
    - "The project MUST use at least one automated test suite…"
    - "At least one static code analysis tool MUST be applied…"
    - "The project MUST publish the process for reporting vulnerabilities on the project site."
  - Form-based approach based on practices of well-run OSS projects
- If OSS project meets best practice criteria, it earns a badge
  - Enables projects & potential users know current status & where it can improve
  - Combination of self-certification, automated checks, spot checks, public accountability
- Three badge levels: **passing**, **silver**, **gold**
- Participation widespread & continuing to grow
  - >7,500 participating projects, >1,400 passing+ (Sep 2024)
  - Current statistics: https://www.bestpractices.dev/en/project_stats
- For more, see: https://www.bestpractices.dev

# OpenSSF Scorecard


- *Automatically* scores OSS projects on heuristics ("checks")
  - Each related to security, scored 0-10, weighted average computed
  - Can use to evaluate your own or others' projects (they don't need to cooperate)
  - Works for projects hosted on GitHub & more recently GitLab
- We routinely run Scorecard on > 1M OSS projects; any can run
- Sample checks (out of 19):
  - Binary-Artifacts — Is the project free of checked-in binaries?
  - Branch-Protection — Does it use Branch Protection?
  - CI-Tests — Does it run tests in CI, e.g. GitHub Actions, Prow?
  - Code-Review — Does it require code review before code is merged?
  - Contributors — Does it have contributors from at least two different organizations?
  - CII-Best-Practices — Does it have an OpenSSF (formerly CII) Best Practices Badge? [next!]
- Sonatype 2022 report found it could help predict likelihood of known vulnerabilities
- https://github.com/ossf/scorecard

# Supply-chain Levels for Software Artifacts (SLSA)




- Focuses on safeguarding artifact integrity across software supply chains
- "Build" and "Package" parts of the SDLC

| Level | Requirements | Focus |
|---|---|---|
| Build L1 | Provenance showing how the package was built | Mistakes, documentation |
| Build L2 | Signed provenance, generated by a hosted build platform | Tampering after the build |
| Build L3 | Hardened build platform | Tampering during the build |

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

https://slsa.dev/

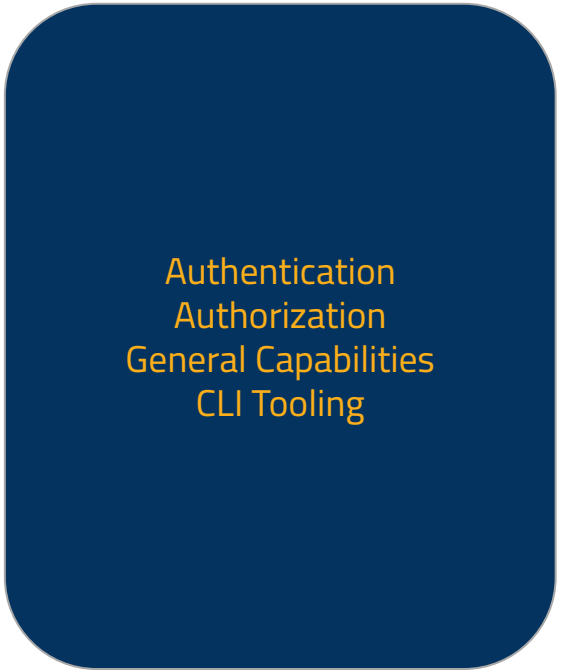
OSS Supplier | OSS Consumer | CISO + Public Sector

# S2C2F

- Guide that outlines how to securely consume OSS dependencies into dev workflows
- Includes a solution-agnostic set of practices and a maturity-model-based implementation guide
- For more, see: https://github.com/ossf/s2c2f/blob/main/README.md

# Principles for Package Repository Security

- A joint community-public sector effort to help identify and encourage the use of security practices at the repo-level so that all projects within that ecosystem can benefit with minimal additional overhead
- 4 Capabilities with 4 levels of security maturity
- https://repos.openssf.org/principles-for-package-repository-security




OpenSSF
OPEN SOURCE SECURITY FOUNDATION

OSS Supplier | OSS Consumer | CISO + Public Sector

# sigstore

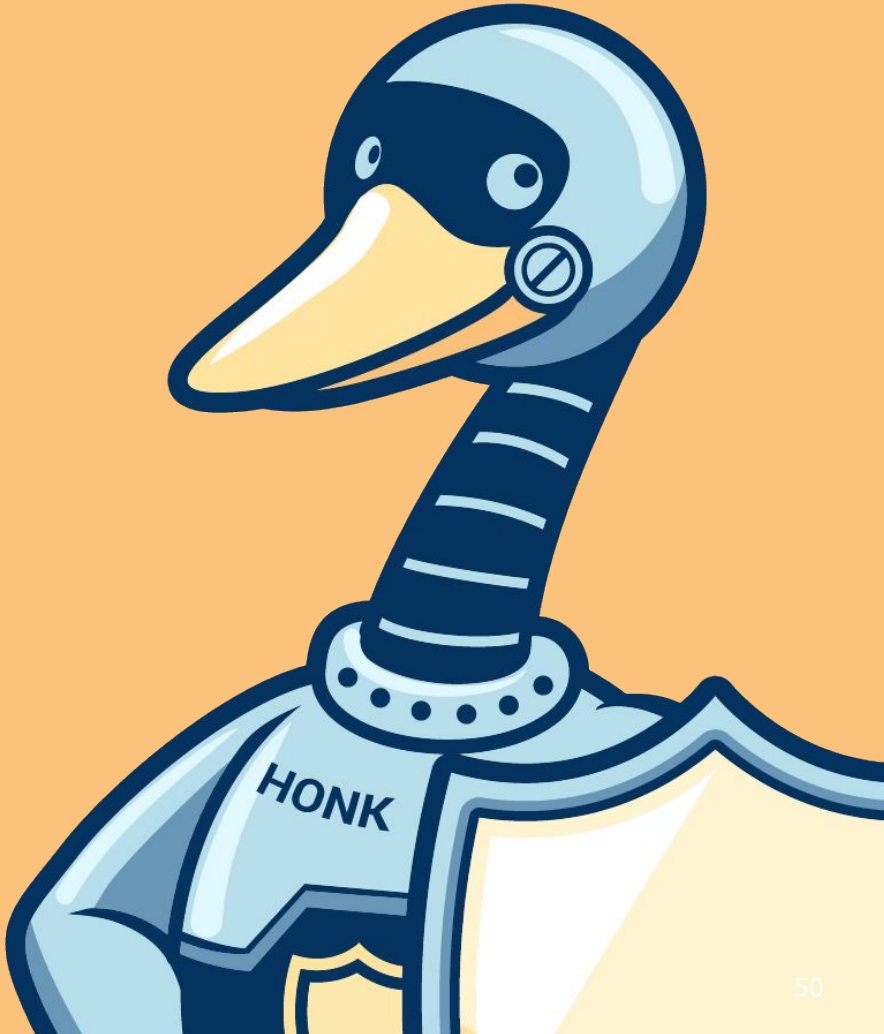
- Sigstore is a new standard for signing, verifying, and protecting software.
- Sigstore enables developers to validate that the software they are using is exactly what it claims to be using cryptographic digital signatures and transparency log technologies.
- Sigstore offers a suite of technologies that include Cosign for signing software artifacts, the Fulcio certificate authority, the Rekor transparency log, and Gitsign for signing Git commits. These tools can be used independently, or as one single process, for a holistic approach to open source security.


OpenSSF
OPEN SOURCE SECURITY FOUNDATION

https://openssf.org/projects/sigstore/

OSS Maintainer | OSS Supplier | OSS Consumer | CISO + Public Sector

# Select text of the CRA



The Text of REGULATION (EU) 2024/284 (the CRA) is presented here to highlight specific cyber security tasks, processes, and tools that will needed to be compliant.

All emphasis (bold, colouring, italics) are added to call out specific actions required.

Slight alterations to the formatting of the text have been made for readability/display on these slides.

r(76)

**Manufacturers** of products with digital elements should put in place coordinated vulnerability disclosure policies to facilitate the reporting of vulnerabilities by individuals or entities either directly to the manufacturer or indirectly, and where requested anonymously, via CSIRTs designated as coordinators for the purposes of coordinated vulnerability disclosure in accordance with Article 12(1) of Directive (EU) 2022/2555. Manufacturers' **coordinated vulnerability disclosure policy** should specify a structured process through which vulnerabilities are reported to a manufacturer in a manner allowing the manufacturer to diagnose and remedy such vulnerabilities before detailed vulnerability information is disclosed to third parties or to the public. Moreover, manufacturers should also consider publishing their security policies in machine-readable format. Given the fact that information about exploitable vulnerabilities in widely used products with digital elements can be sold at high prices on the black market, manufacturers of such products should be able to use programmes, as part of their coordinated vulnerability disclosure policies, to incentivise the reporting of vulnerabilities by ensuring that individuals or entities receive recognition and compensation for their efforts. This refers to so-called 'bug bounty programmes'.

r(77)

In order to facilitate vulnerability analysis, manufacturers should identify and document components contained in the products with digital elements, including by drawing up an SBOM. An SBOM can provide those who manufacture, purchase, and operate software with information that enhances their understanding of the supply chain, which has multiple benefits, in particular it helps manufacturers and users to track known newly emerged vulnerabilities and cybersecurity risks. It is of particular importance that manufacturers ensure that their products with digital elements do not contain vulnerable components developed by third parties. Manufacturers should not be obliged to make the SBOM public

# Article 13

3. The **cybersecurity risk assessment** shall be documented and updated as appropriate during a support period to be determined in accordance with paragraph 8 of this Article. That cybersecurity risk assessment shall comprise at least an analysis of cybersecurity risks based on the intended purpose and reasonably foreseeable use, as well as the conditions of use, of the product with digital elements, such as the operational environment or the assets to be protected, taking into account the length of time the product is expected to be in use. The cybersecurity risk assessment shall indicate whether and, if so in what manner, the security requirements set out in Part I, point (2), of Annex I are applicable to the relevant product with digital elements and how those requirements are implemented as informed by the cybersecurity risk assessment. It shall also indicate how the manufacturer is to apply Part I, point (1), of Annex I and the vulnerability handling requirements set out in Part II of Annex I.

6. **Manufacturers** shall, **upon identifying a vulnerability in a component**, including in an open source-component, which is integrated in the product with digital elements report the vulnerability to the person or entity manufacturing or maintaining the component, and address and remediate the vulnerability in accordance with the vulnerability handling requirements set out in Part II of Annex I. Where manufacturers have developed a software or hardware modification to address the vulnerability in that component, they shall share the relevant code or documentation with the person or entity manufacturing or maintaining the component, where appropriate in a machine-readable format.

# Article 13, cont.

8. **Manufacturers** shall ensure, when placing a product with digital elements on the market, and for the support period, that vulnerabilities of that product, including its components, are handled effectively and in accordance with the essential cybersecurity requirements set out in Part II of Annex I.

Manufacturers shall determine the support period so that it reflects the length of time during which the product is expected to be in use,

…

Without prejudice to the second subparagraph, the support period shall be at least five years. Where the product with digital elements is expected to be in use for less than five years, the support period shall correspond to the expected use time.

9. **Manufacturers** shall ensure that each security update, as referred to in Part II, point (8), of Annex I, which has been made available to users during the support period, remains available after it has been issued for **a minimum of 10 years** or for the remainder of the support period, whichever is longer

# Article 14

1. A **manufacturer** shall notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to **ENISA**. The manufacturer shall notify that actively exploited vulnerability via the single reporting platform established pursuant to Article 16.

2. For the purposes of the notification referred to in paragraph 1, the manufacturer shall submit:

(a) an early warning notification of an actively exploited vulnerability, without undue delay and in any event within **24 hours** of the manufacturer becoming aware of it, indicating, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available;

(b) unless the relevant information has already been provided, a vulnerability notification, without undue delay and in any event within **72 hours** of the manufacturer becoming aware of the actively exploited vulnerability, which shall provide general information, as available, about the product with digital elements concerned, the general nature of the exploit and of the vulnerability concerned as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take, and which shall also indicate, where applicable, how sensitive the manufacturer considers the notified information to be;

(c) unless the relevant information has already been provided, a **final report, no later than 14 days after** a corrective or mitigating measure is available, including at least the following:

(i) a description of the vulnerability, including its severity and impact;

(ii) where available, information concerning any malicious actor that has exploited or that is exploiting the vulnerability;

(iii) details about the security update or other corrective measures that have been made available to remedy the vulnerability;

# Article 14, cont.

8. After becoming aware of an actively exploited vulnerability or a severe incident having an impact on the security of the product with digital elements, the manufacturer shall inform the impacted users of the product with digital elements, and where appropriate all users, of that vulnerability or incident and, where necessary, of any risk mitigation and corrective measures that the users can deploy to mitigate the impact of that vulnerability or incident, where appropriate **in a structured, machine-readable format that is easily automatically processable.** *Where the manufacturer fails to inform the users of the product with digital elements in a timely manner, the notified CSIRTs designated as coordinators may provide such information to the users when considered to be proportionate and necessary for preventing or mitigating the impact of that vulnerability or incident.*

# Article 16

1. For the purposes of the notifications referred to in Article 14(1) and (3) and Article 15(1) and (2) and in order to simplify the reporting obligations of manufacturers, **a single reporting platform shall be established by ENISA**. The day-to-day operations of that single reporting platform shall be managed and maintained by ENISA. The architecture of the single reporting platform shall allow Member States and ENISA to put in place their own electronic notification end-points.
2. After receiving a notification, the CSIRT designated as coordinator initially receiving the notification shall, without delay, disseminate the notification via the single reporting platform to the CSIRTs designated as coordinators on the territory of which the manufacturer has indicated that the product with digital elements has been made available.

# Article 17

5. After a security update or another form of corrective or mitigating measure is available, ENISA shall, in agreement with the manufacturer of the product with digital elements concerned, add the publicly known vulnerability notified pursuant to Article 14(1) or Article 15(1) of this Regulation to the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555.

# ANNEX 1

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.

# ANNEX 1, cont.

(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:

(a) be made available on the market without **known exploitable vulnerabilities**;

(b) be made available on the market with **a secure by default configuration**, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;

(c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;

(d) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;

(e) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means;

(f) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;

(g) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation);

# ANNEX 1 (2) cont.

(h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;

(i) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;

(j) be designed, developed and produced to **limit attack surfaces**, including external interfaces;

(k) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

(l) provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user;

(m) provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.

# ANNEX 1 cont. Part II Vulnerability handling requirements

**Manufacturers** of products with digital elements shall:

(1) identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a **software bill of materials** in a commonly used and machine-readable format **covering** at the very least the **top-level dependencies** of the products;

(2) in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

(3) apply effective and regular tests and reviews of the security of the product with digital elements;

(4) once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;

(5) put in place and enforce a **policy on coordinated vulnerability disclosure**;

(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, **where applicable for security updates, in an automatic manner**;

(8) ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

# ANNEX II

At minimum, the product with digital elements shall be accompanied by:

1. the name, registered trade name or registered trademark of the manufacturer, and the postal address, the email address or other digital contact as well as, where available, the website at which the manufacturer can be contacted;

2. the **single point of contact** where information about vulnerabilities of the product with digital elements can be reported and received, and where the **manufacturer's policy on coordinated vulnerability disclosure** can be found;

3. name and type and any additional information enabling the unique identification of the product with digital elements;

4. the intended purpose of the product with digital elements, including the security environment provided by the manufacturer, as well as the product's essential functionalities and information about the security properties;

5. any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;

6. where applicable, the internet address at which the EU declaration of conformity can be accessed;

# ANNEX II, cont.

7. the type of technical security support offered by the manufacturer and the end-date of the support period during which users can expect vulnerabilities to be handled and to receive security updates;

8. detailed instructions or an internet address referring to such detailed instructions and information on:

(a) the necessary measures during initial commissioning and throughout the lifetime of the product with digital elements to ensure its secure use;

(b) how changes to the product with digital elements can affect the security of data;

(c) how security-relevant updates can be installed;

(d) the secure decommissioning of the product with digital elements, including information on how user data can be securely removed;

(e) how the default setting enabling the **automatic installation of security updates**, as required by Part I, point (2)(c), of Annex I, can be turned off;

(f) where the product with digital elements is intended for integration into other products with digital elements, the information necessary for the integrator to comply with the essential cybersecurity requirements set out in Annex I and the documentation requirements set out in Annex VII.

9. If the manufacturer decides to make available the software bill of materials to the user, information on where the software bill of materials can be accessed.