Cybersecurity Strategy in the Face of Global Digital Regulation

Christopher “CRob” Robinson
Chief Technology Officer/Chief Security Architect - OpenSSF/Linux Foundation

LF Europe Roadshow 2025

October 29, 2025

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Who is this guy?

CRob, n, adj, and v

Pronunciation: U.S. (K-rowb)

```
# chmod 666 crob.md
```

44th level Dungeon Master

27th level Securityologist

Pirate-enthusiast & hat-owner

Chief Technology Officer & Chief Security Architect, OpenSSF - Linux Foundation

Involved in upstream OSS CVD for ~15 years

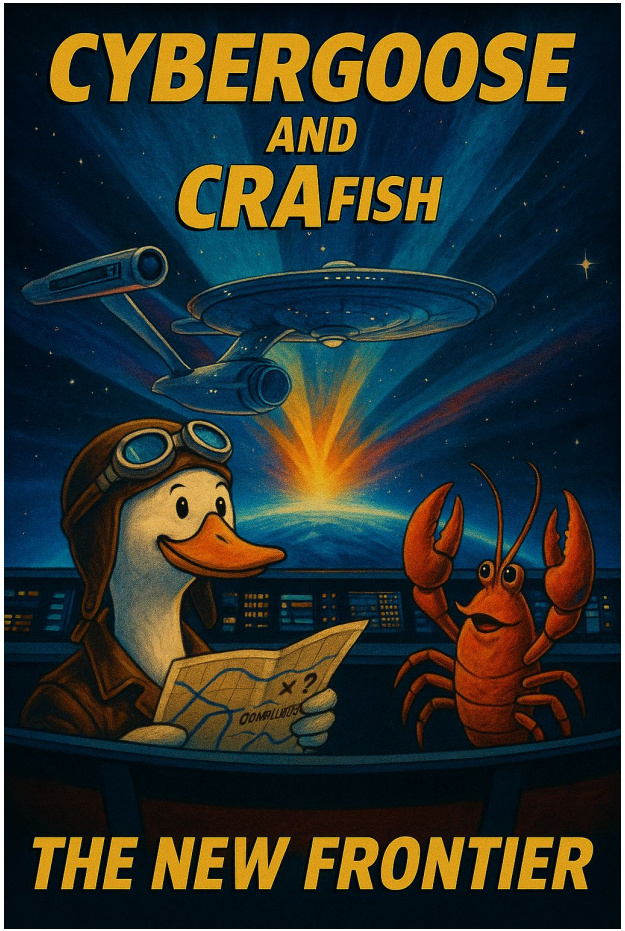
Recovering Super-Regional Bank Tech Eng/Ops Manager

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

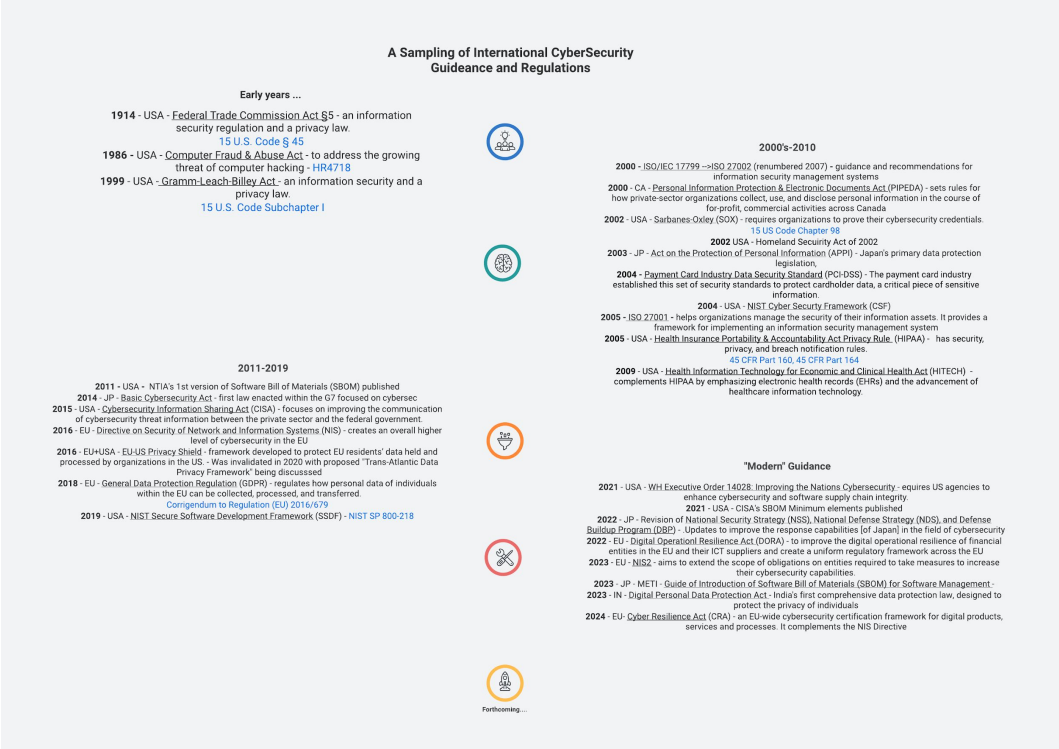
Most images generated by ChatGPT, except that -> That's just my pal Gimp!

Setting the Stage: The New Frontier

- Digital regulation is converging across continents.
- Cybersecurity strategy must shift from reactive compliance to evidence-based assurance.
- This talk traces the journey from historic laws to the CRA.



Welcome to the awesome World of Global CyberSecurity Compliance



Our topic today has DEEP international roots in both legislation and case-law dating back to 1914.

Let's zoom in on a few touchstone frameworks and regulations that have accelerated the need for us to collaborate more than ever before....

Global Cyber Law Timeline

Regulation / Framework	Adoption / Entry into Force	Key Application / Enforcement Dates
NIST CSF v1.0	February 2014	–
GDPR	Adopted 2016 → applied 25 May 2018	2018 enforcement
U.S. EO 14028	May 2021	Software supply-chain measures 2021–2022
ISO/IEC 27001:2022	Published Oct 2022	Transition by Oct 31 2025
NIS2 Directive	Adopted Dec 2022 → in force Jan 2023	Member-state transposition by 17 Oct 2024
NIST SSDF v1.1	Feb 2024	Immediate reference in U.S. gov procurement
DORA	In force Jan 2023	Applies 17 Jan 2025
EU AI Act	Adopted 2024	Bans Feb 2025 · GPAI Aug 2025 · High-risk 2026/27
Cyber Resilience Act (CRA)	**Entered into force 10 Dec 2024**	**Applies from 11 Sep 2026 → full obligations 11 Dec 2027**

The Inflection Point

Voluntary → Mandatory

Privacy → Product Safety

Policy → Evidence

Your Compass: Core Frameworks

- NIST CSF 2.0 → Governance
- NIST SSDF v1.1 → Secure Development Lifecycle
- ISO 27001 (2022) → ISMS modernization
- IEC 62443 → Industrial/OT focus

The European Terrain

- NIS2: Accountability & supply-chain oversight (Oct 2024)
- DORA: ICT resilience for financial entities (Jan 2025)
- AI Act: Risk-based obligations & transparency (Aug 2025 onward)

The Cyber Resilience Act (CRA)

- Effective Dec 2024; duties apply Dec 2027
- Covers “Products with digital elements”
- CE marking now includes cybersecurity assurance
- Secure-by-design, vulnerability handling, and post-market duties

CRA Reporting Clock

Severe Incidents and Exploited Vulnerabilities

24h – Early Warning to CSIRT/ENISA
72h – Incident/Vulnerability notification
1 Month – Final report

Mapping CRA & NIS2 to NIST SSDF

SSDF → CRA/NIS2 Mapping:

- PO (Planning & Governance) → Executive accountability
- PS (Security Requirements) → Secure-by-design architecture
- PW (Implementation & Verification) → CE documentation & testing evidence
- RV (Response & Monitoring) → CVD policy & post-market duties

What is the Baseline?

Est. 2024

The OpenSSF's Open Source Project Security Baseline (OSPS Baseline or simply "Baseline") refers to a collection of efforts led by the OpenSSF in collaboration with members and LF partners (CNCF, FINOS, OpenJS, and more!).

The Baseline includes a Catalog of requirements that map to industry standards, frameworks, and regulations, and Tooling to assist in determining Baseline-compliance, that automate Baseline configuration settings, and links to evidence and attestations.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

All your Base are belong to us

https://openssf.org/press-release/2025/02/25/openssf-announces-initial-release-of-the-open-source-project-security-baseline/

https://www.youtube.com/watch?v=DxiYI79SIIg

The OpenSSF Security Baseline was officially released Feb 2025

Based on a library of well-known cybersecurity frameworks, standards, and global regulations

It includes **40** requirements across **3** levels of maturity covering **8** areas of cyber and application security practices

- Access Control
- Build & Release
- Documentation
- Governance
- Legal
- Quality
- Security Assessment
- Vulnerability Management

The criteria range from simple things like documenting processes and procedures to more complex tasks such as infrastructure configuration, all related to SDLC and modern software engineering practices

https://baseline.openssf.org
https://github.com/ossf/security-baseline
https://github.com/ossf/wg-ORBIT

Building a Better Catalog

Baseline currently maps alignment across multiple cyber compliance frameworks and/or cyber legislations. "Baselining" helps downstream select projects that align with and that support their compliance obligations!

NIST National Institute of Standards and Technology U.S. Department of Commerce

- SSDF
- CSF
- 800-161/800-53
- CISA Software Acquisition Guide (forthcoming)

European Commission

- Cyber Resilience Act
- DORA (forthcoming)
- NIS2 (forthcoming)

National Cyber Security Centre a part of GCHQ

- Software Security Code of Practice (forthcoming)

OpenSSF OPEN SOURCE SECURITY FOUNDATION

- BP Badges
- Scorecard
- Minder
- SLSA
- OpenSSF tooling

PCI Security Standards Council

SAMM

OPENCRE

OPENCHAIN

Proactive Software Supply Chain Risk Management (P-SSCRM) Framework

Have a framework or a particular piece of legislation you'd like to see integrated into the Baseline? Patches Welcome!

Expedition Kit: 2025+ Strategy

1. CRA gap assessment vs SSDF
2. Product Security/CVD office
3. Automate evidence generation (SBOMs, test results)
4. CE technical documentation templates
5. Supplier alignment (DORA/NIS2)
6. 24/72h drill rehearsals

Regional Hazards Map

The regulatory terrain varies by regional market and vertical.

Map obligations early to prevent being blindsided.

From Compliance to Confidence

"Security isn't the map—it's the journey we take together."

- Regulations are synchronizing across continents.
- SSDF and CRA define the new standard of trust.
- Build culture, evidence, and resilience now.

Thank You

CRob_at_OpenSSF_dot_org

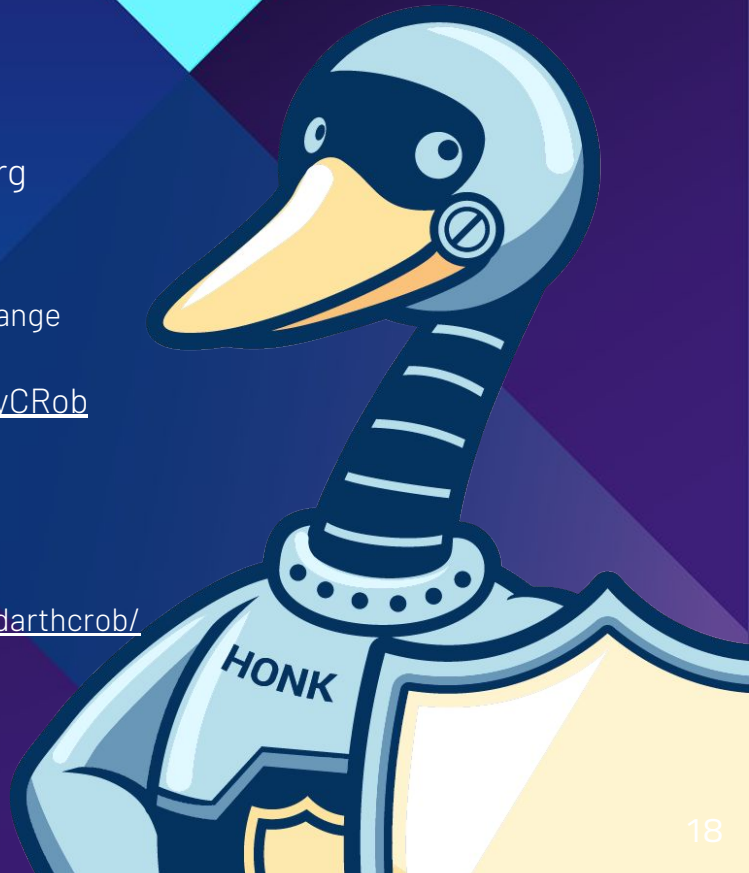
@~~SecurityCRob~~

@SecurityCRob@infosec.exchange

https://github.com/SecurityCRob

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

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



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Legal Notice

CYBERSECURIT STRATEGY IN THE FACE OF GLOBAL DIGITAL REGULATION

From voluntary guidance to enforceable secuity-by-ign

Christopher "CRob" Robinson
Chief Technology Officer/Chief Security Architect - OpenSSF/Linux Foundation

LF Europe Roadshow 2025

October 29, 2025