



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



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

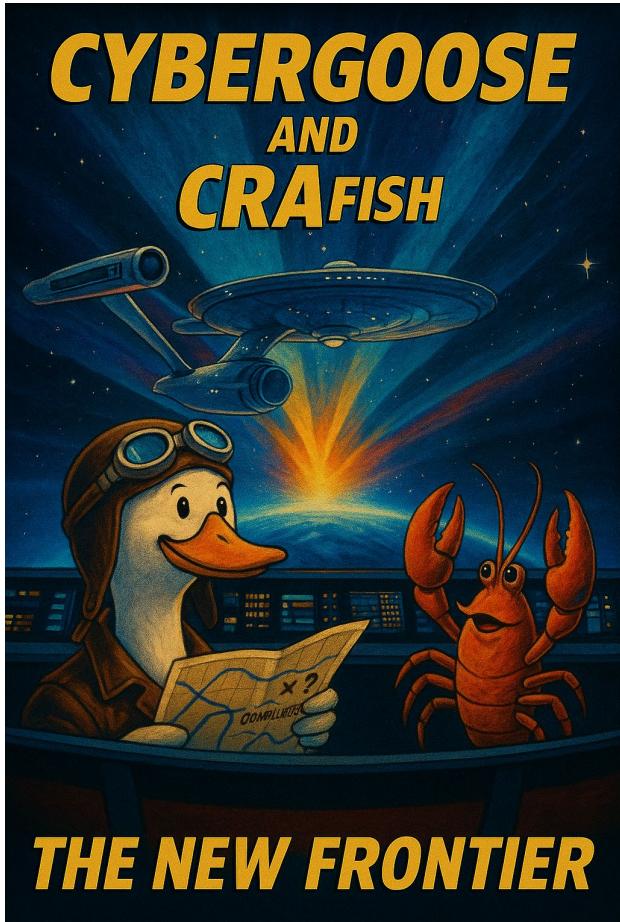
Recovering Super-Regional Bank Tech Eng/Ops Manager



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

A Sampling of International CyberSecurity Guidance 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 27001 (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 companies to prove their cybersecurity credentials
15 U.S. Code Chapter 9E

2002 USA - Homeland Security Act of 2002

2003 - JP - Act on the Protection of Personal Information (APPPI) - 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 - NIST Cyber Security Framework (CSF) - 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

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

"Modern" Guidance

2021 - USA - WH Executive Order 14028, Improving the Nation's Cybersecurity - requires US agencies to enhance cybersecurity and software supply chain integrity

2021 - USA - OSA's 590M 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 Operational Resilience Act (DORA) - to improve the digital operational resilience of financial entities in the EU and their ICT suppliers, and to unify the 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



2011-2019

2011 - USA - NTIA's 1st version of Software Bill of Materials (SBOM) published

2014 - JP - Basic Cybersecurity Act - first law enacted within the G7 focused on cybersecurity

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 discussed

2018 - EU - General Data Protection Regulation (GDPR) - 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



Forthcoming ...

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

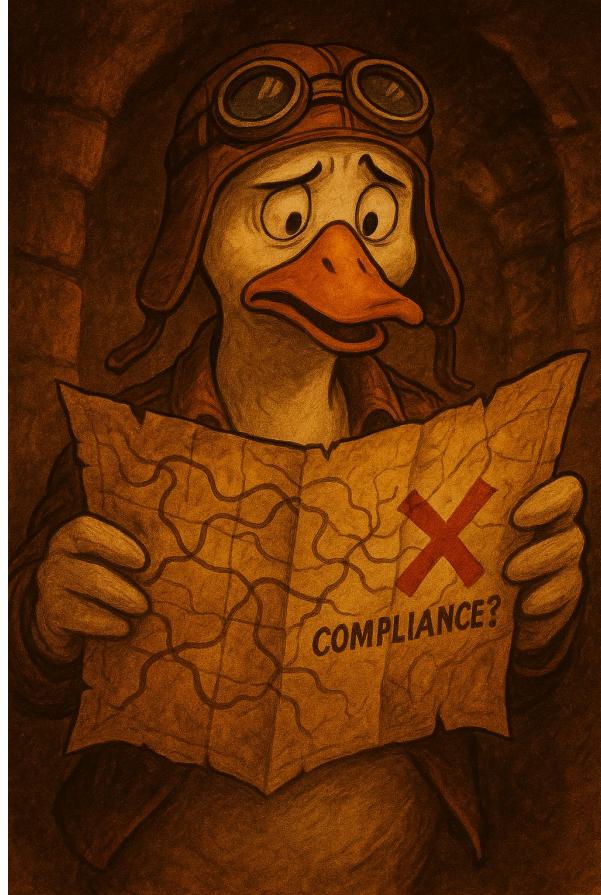
1 Month – Final report



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.

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/>

A YouTube thumbnail for a video titled "How to Use Open Source Project Security Baseline to Better Navigate Standards & Regulations?". It features a grid of four video feeds showing people in a video conference. Below the title, it says "Tech Talk | Thur. April 24, 2PM ET". The OpenSSF logo is at the bottom.

<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!



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



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



National Cyber Security Centre
a part of GCHQ

- Software Security Code of Practice (*forthcoming*)



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



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/>



Legal Notice

Copyright © [Open Source Security Foundation](#)®, [The Linux Foundation](#)®, & their contributors. The Linux Foundation has registered trademarks and uses trademarks. All other trademarks are those of their respective owners.

Per the [OpenSSF Charter](#), this presentation is released under the Creative Commons Attribution 4.0 International License (CC-BY-4.0), available at <<https://creativecommons.org/licenses/by/4.0/>>. You are free to:

- Share — copy and redistribute the material in any medium or format for any purpose, even commercially.
- Adapt — remix, transform, and build upon the material for any purpose, even commercially.

The licensor cannot revoke these freedoms as long as you follow the license terms:

- Attribution — You must give appropriate credit , provide a link to the license, and indicate if changes were made . You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

CYBERSECURITY STRATEGY

IN THE FACE OF

GLOBAL DIGITAL REGULATION

From voluntary guidance to enforceable security-by-design

Christopher "CRob" Robinson

Chief Technology Officer/Chief Security Architect - OpenSSF/Linux Foundation

LF Europe Roadshow 2025

October 29, 2025

