



Secure Code Is Critical Infrastructure Hacking Policy for Public Good

Tanya Janca

#SECTORCA @BlackHatEvents

What are we going to talk about today?

What happens when a private citizen
wants their government to improve their
software security.

Hint: it's *a journey* !

What YOU can do to get YOUR
government to improve.

And how you can help me with mine. :-D

Plus:
A copy of the secure coding policy!

Tanya Janca



- Secure Coding Trainer at SheHacksPurple Consulting
- Author: Alice and Bob Learn Secure Coding & Alice and Bob Learn Application Security
- 28+ years in tech, Sec + Dev
- Founder: We Hack Purple, OWASP DevSlop, #CyberMentoringMonday, WoSEC
- Advisor: Smithy, Katilyst
- Contributor: OWASP Top Ten, StackOverflow
- Board Member: Forte Group

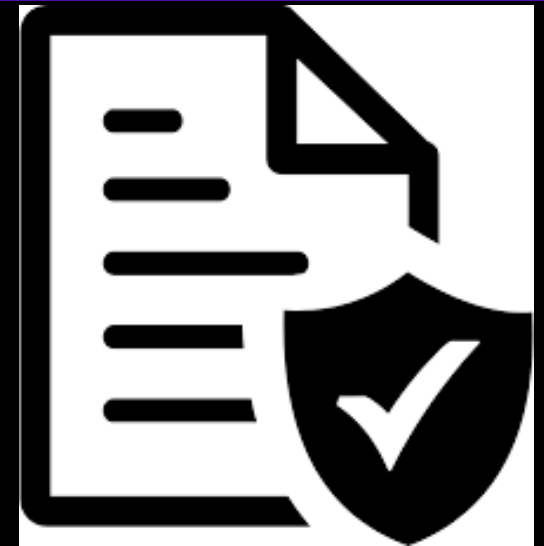
The mandatory 'about' me slide.



She seems
tolerable!

Let's Talk Policy

And why it matters.



Why Policy Matters

- Insecure code = national risk
- Secure code protects democracy, privacy, and public safety
- Devs are graduating without ever learning secure coding
- Vibe coding and AI is NOT helping



POLICY IS IMPORTANT

- Offers guidance
- Something to hold people accountable to
- Helps us secure critical infrastructure



The Current Security Landscape in Canada

* According to Tanya and the internet, *not* inside sources

Current Landscape



- The Canadian Public Service does not have a formal secure coding policy they must follow*
- No government wide, public vulnerability/ responsible disclosure program or bug bounty
- No government wide-education on this topic
- Limited online guidance available from CCCS

Current Guidance



- Software Security Code of Practice cyber.gc.ca CCCS
- Not mandatory
- Only 4 items refer to secure coding
- Briefly covers secure SDLC and 'secure by design'
- Generally vague/high level, mostly not actionable
- Focuses on processes over details

Current Guidance



- Security Considerations When Using Open-Source Software (ITSAP-10059)
- Not mandatory
- Suggests SBOM but not Software Composition Analysis, no automation or scaling suggested
- Generally, pretty good advice, if incomplete

Current Guidance



- Protecting Your Organization from Software Supply-Chain Threats (ITSM-10071)
- Not mandatory
- Better advice, more thorough
- Still no SCA, scaling or automation suggestions

Current Guidance



- Security considerations for your website (ITSM.60.005)
- Very basic guidance, but accurate
- For the public, not the government
- Better than nothing!
- Doesn't even meet my 'MVS' standard

The Issue: (according to Tanya)



- It's not that they are not working hard
- It's not that there are not *many* smart people involved
- It's that they are NOT focusing on software, and software runs our country
- We have 1.3 million tech workers*, with no guidance
- Over half of that 1.3M are devs

Current Strategy (2025)



- **Public-Private Partnerships**
- **Cyber Security Certification:** They test them against NIST, which covers some S-SDLC, but no secure coding.
- **Consumer Protection:** Exploration of IoT labeling and cyber security certifications to inform and protect consumers.
- **Research and Talent Development:** Investment in the Cybersecurity Attribution Data Centre (CADC) to advance AI-driven cyber analytics and train specialists. Not secure coding.

Current Strategy (2025)



- They are doing a lot
- But I don't feel they are covering secure software
- And by "feel" I mean I don't see it anywhere in the documents and research I have done
- I would enjoy being proven wrong
- Seriously, please correct me after I'm wrong.

Constant Breaches - CRA



- 2020 Credential Stuffing Attacks
- 2020 GCKey Attack
- 2020 Unauthorized Access via Stolen Credentials
- 2020 Internal Data Breach
- 2025 The CRA Admits Underreporting Massive Cyber Breaches Impacting Tens of Thousands of Canadians – article
- There is also a class action lawsuit against them for negligence
- **They lost 2 of my parent's identities**
- Their terms of service are abysmal, yet it's illegal to not use their service
- I tried CRA for years, but now focus on entire government after stonewalling

Constant Breaches - GC



- The rest of the Canadian Federal government isn't that much better
- Chinese State-Sponsored Cyberattacks (2019–2023)
- Statistics Canada Breaches (2022–2023)
- Royal Canadian Mounted Police (RCMP) Data Breach (2020)
- Global Affairs (2022 -2024)
- There's so much more they are not telling us. They only have to report 'material' or citizen privacy breaches, the rest remains secret.
- I am unable to comment on what I experienced during my 13.5 years of service.
- I left the GC February 2018.

What I have done to further security since departing the Public Service.

Tanya's Efforts

(personal action)



- I've been volunteering with the ICTC since 2018 to add 'cyber' to high school and primary school curriculum (Information and Communications Technology Council)
- I'm the 'ethical hacker' lesson in one of our national textbooks that covers careers
- I have arranged for security professionals across Canada to go to schools for career day
- I have helped to promote and support funding for Cyber Titan and other high school educational initiatives that involve cyber
- I have guest lectured for free across the country at universities and colleges
- I made my online academy content free, worldwide (Semgrep academy)



what happened
when I went public?

Absolutely nothing.

Tanya's Efforts

(lobbying)



- Contacted CRA about their terrible terms of service and the fact that they are not following their web app security policy (which I wrote when I worked for them, it is not publicly available)
- Wrote letters to the prime minister's office when CRA would not answer
- Wrote a blog post, they did not response
- Wrote a post for Risky business blog, no response <https://risky.biz/risky-biz-news-canadas-tax-revenue/>
- Posted on social media
- Gave a speech on this topic at the Privacy and Access Council of Canada, knowing members of the CRA team would be there

Tanya's Efforts

(lobbying)



- Tried back channels, including confronting the CIO in person at a conference in Ottawa (respectfully and politely)
- Wrote a practical, cost-effective secure coding policy, offering it free
- Worked with my MP to propose policy for public servants, with a joint letter writing campaign to ministers from Shared Services and Public Safety
- Attempted to work with my new MP Jeff Kibble, ignored so far
- More letters to Minister of National Security (military), Minister of Shared Services, Public Safety, and the Privacy Commissioner of Canada.
- Approached The Treasury Board Secretariat and Canadian Centre for Cyber Security (CCCS) at B-Sides Ottawa (November 2024), it also went no where.

Tanya's Efforts

(lobbying)



- Spoke on the main stage at Def Con about it in Vegas, Aug 2025, now SecTor in Toronto
- Wrote even more letters:
- Treasury Board Secretariat (TBS)
- Canada Revenue Agency - CRA
- CSEC
- Shared Services
- Department of Defense
- Public Services and Procurement Canada (PSPC)
- Privacy Commissioner
- MPs: Jeff Kibble (multiple times), Katrina Gould, Jean-Yves Duclos, David McGuinty

The Policy

What the Policy Includes

- 9 pages of actionable advice for any software developer
- The guidance is agnostic, meaning it applies to any language, framework, cloud or tech stack
- QR Code & Link

SecureCodingGuideline.com



What YOU Can Do

What YOU Can Do



- Contact your officials, no matter your country
- Use my policy as a template to suggest change
- Use my template letter to contact your government
- Push for education reform (colleges/ universities)
- Apply pressure publicly when institutions stonewall
- Use social media to tell everyone how you feel



Help Me Petition

- Help me find a Canadian MP who will support my House of Commons petition
- If you are Canadian, sign my iPetition:



The Letter



The Policy



The Petition





Free Secure Coding Guideline and Policy

[https://links.
shehackspurple.ca/
SCpolicy](https://links.shehackspurple.ca/SCpolicy)



@SheHacksPurple

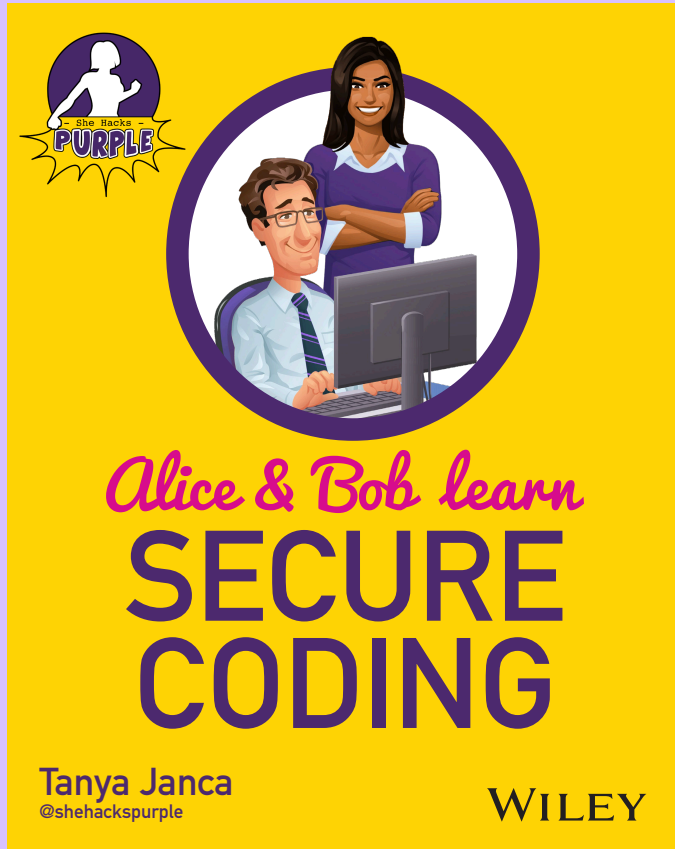
Conclusion

We Learned:

1. Why Security Policy Matters
2. The current security policy in Canada *
3. The poor security landscape of Canada *
4. What I have done to help
5. What you can do to help
6. A free copy of the policy and templates

Resources





My books!





JOIN THE
SHE HACKS PURPLE
Free Monthly Secure
Coding Newsletter
Sign up now!

Newsletter.SheHacksPurple.ca

Sign my Petition to Secure Canada's Code!



SECURE CANADA'S FUTURE: ADOPT A FEDERAL SECURE CODING POLICY





The Template



The Policy



The Petition

THANK YOU

Presentation Slides ->



Follow me



Learn From Me

Tanya Janca
SheHacksPurple.ca

