Canadian Nuclear Laboratories | Laboratoires Nucléaires Canadiens

Continuous Vetting and the Challenges of Expanded Access to Information

Audrey Crowe

Program Manager
National Security & Critical Infrastructure Research Directorate

March 2026

Agenda

- Importance of continuous vetting
- The importance of continuous vetting for RAD licensees
- Case study – The illegitimate IT remote workforce
  - Who, what, where, when, why?
  - How?
  - Why does this case study matter to radiological security?
- Challenges associated with expanded access to information
  - Security challenges
  - Organizational challenges
- Considerations for path forward
- Discussion

Importance of Continuous Vetting through Employment Lifecycle

Importance of Continuous Employee Vetting

Threat landscape - When traditional vetting practices no longer suffice

- **Amplification of the threat landscape**

Increased means, motives, opportunities

  - Digital transformation of enterprise and operational processes & emergence of remote work
  - Access to information, and democratization of powerful technologies (AI)
  - Economic uncertainty & geopolitical tensions

- **Transformation of the threat landscape**

Malicious actors are increasingly employing converging and blended methods to achieve their objectives [1]

  - Converging: threat actor collaboration (conventional and cybercriminal organizations, extremist groups, malicious insiders, state-actors, even corporations)
  - Blended: cyber and physical capabilities
  - Objectives: financial, ideological, geopolitical or self-motivated

Insiders are the most prominent access vector for these attacks [1]

Importance of Continuous Vetting for RAD Licensees

Continuous Vetting for RAD Licensees

Why would threat actors be interested in rad sources licence holders?

- **More vulnerable**

Rad license holders are typically less stringently regulated than their nuclear power or nuclear fuel supply chain counterparts due to lesser perceived risk

- **Still valuable!**

Access to rad license holders digital and physical environments would provides threat actors with the opportunity to :

- Illegally acquire radiological materials (radiological dispersal devices or radiological exposure devices)
- Acquire coercive leverage through operational disruptions (sabotage)
- Achieve financial gains through operational disruptions (ransomware or extorsion)
- Illegally acquire intellectual property and proprietary information to advance malicious capabilities (controlled technologies)

CASE STUDY

The Illegitimate IT Remote Workforce

Who, What, Where, When, Why

Who	Nation State-Actor
What	Implanted 3,000-10,000* remote operatives as employees in [2]
Where	• Globally, many Fortune 500 companies affected [3] • Targets supply chain: professional services consulting (IT, cybersecurity, engineering), software and emerging technology development. • Increased occurrences in health care and finance sectors
When	Since mid-2010's – Ongoing
Why	• Financial Gain (employment & extorsion) • Acquire IP (controlled technologies) • Acquire sensitive information (lay of the land, credentials, etc.) • Establish foothold for future attacks

*AI-Generated Image, Microsoft Copilot 25 February 2026

HOW

Malicious actors **leveraged accessible information** online from social media, conventional & dark web, along with **AI tools** to:

Secure Interview
- Generate false resumes, professional credentials & social media accounts

Complete Interview Process
- Modify appearance in real-time with deepfakes using stolen biometrics
- Successfully answer technical interview questions in real-time using LLM

Complete Onboarding Process
- Establish legitimate yet fraudulent social and financial credentials
- Domestic insiders support false employment verification

Operational Support
- Recruit & communicate with domestic insiders to facilitate operations via social media or communications platform

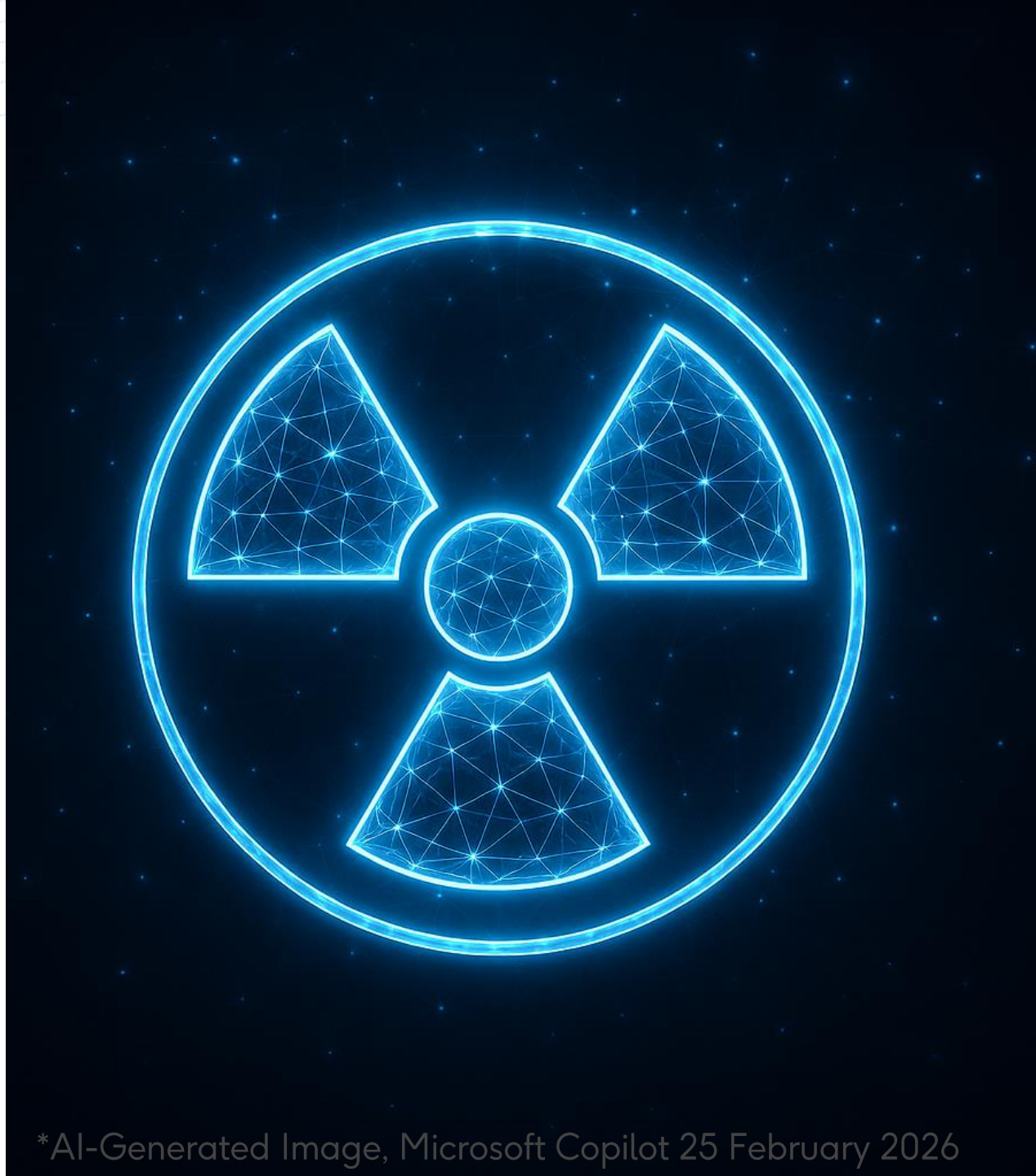
Result: Malicious insider gained legitimate yet fraudulent access to organization's and, in some cases, their clients' digital environment

Implications: Ability to compromise the confidentiality, integrity & availability of both digital and physical information, systems, and materials

Why does this case study matter to RAD Licence Holders?

The case study shows how expanded access to information and publicly available emerging technology can:

- Increase the risk of unknowingly hiring or contracting unqualified or illegitimate workers
- Increase the risk of procuring compromised software & applications
- Increase your employees, vendors and collaborator's exposure to exploitation, recruitment or coercion from external threat actors



*AI-Generated Image, Microsoft Copilot 25 February 2026

Challenges Associated with Expanded Access to Information

Security Challenges

Amplification of threats and severity of compromise

Expanded access to information, especially when combined with AI [4] :

Increases the number of threat actors, their activities & their sophistication

- Rapid upskilling - Sectors previously “off-limit” due to technical complexity are now broadly accessible
- Automation of cyberoperations
- Rapid development of advanced social engineering tactics – Synthetic identities, deepfakes, fraudulent social media accounts)

Increases severity of compromise

- Threat convergence & blended attacks

Organizational Challenges

Expanded access to information organizational challenges and opportunities

RAD license holders' state of readiness

- Less stringent regulatory requirements
- Security culture
- Resource availability
- Threat awareness

Emergence of OSINT & AI-supported continuous vetting and investigations

- Ethical considerations
- Legal considerations

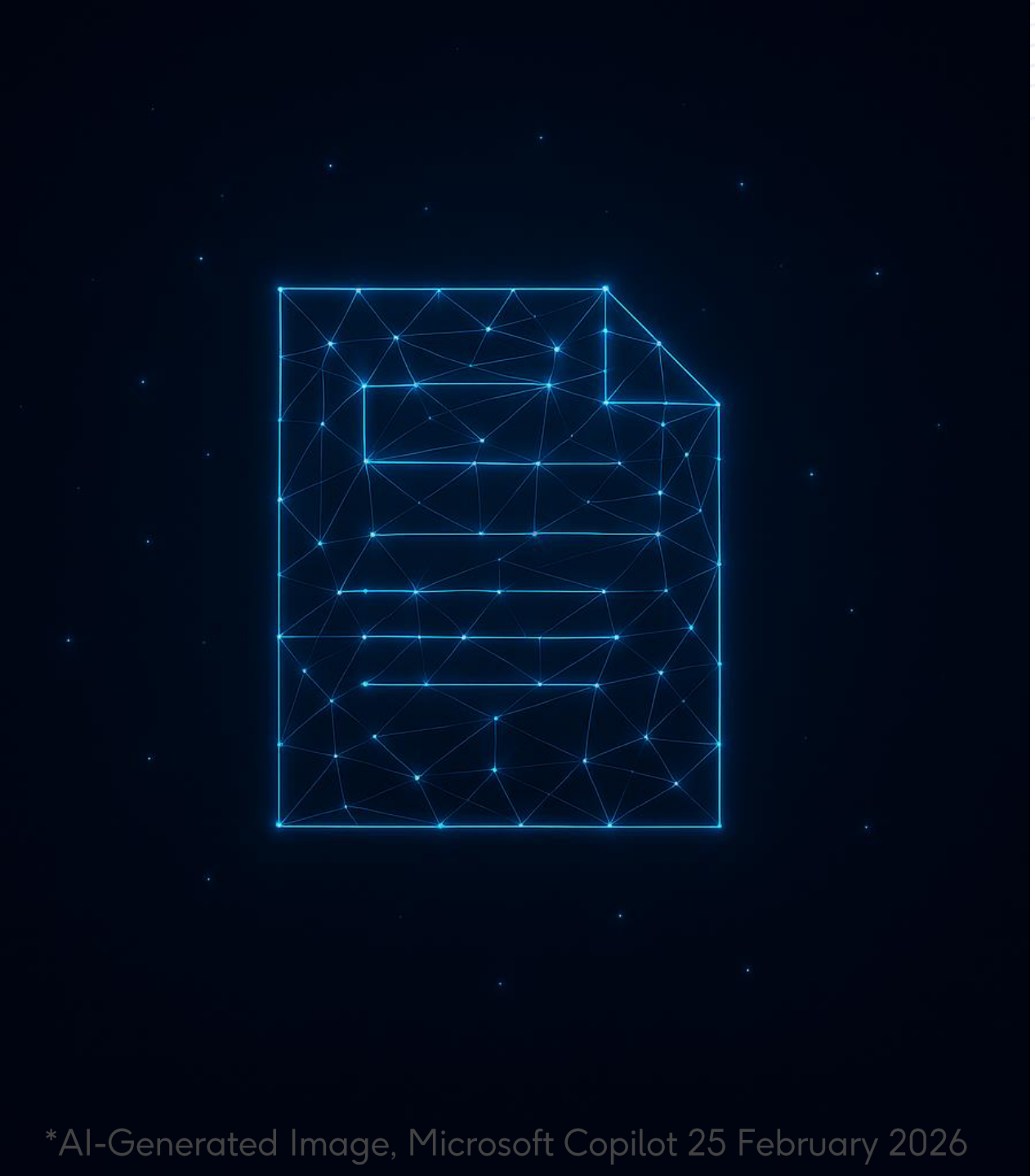
Considerations for Path Forward

Striking the right balance

Adapting best practices to licensee's environment and threat landscape

- Increase organization's threat awareness
  - Threat awareness champion
  - Webinars, lunch and learns, case studies
- Enhance initial vetting practices
  - Account for enduring and emerging social engineering tactics
  - Secondary validation of credentials
- Adopt a risk-based approach to ongoing vetting
  - Align vetting efforts with digital and physical access & knowledge of sensitive information

*AI-Generated Image, Microsoft Copilot 25 February 2026



*AI-Generated Image, Microsoft Copilot 25 February 2026

References

[1] Crowe, Audrey. (2026). “Mass Insider Threats - Civilians, Critical Infrastructure, and the Erosion of Sovereignty in the Grey-Zone”. In *Oxford Intersections: Borders.* Ed. Alexander Diener and Joshua Hagen. Oxford University Press. [Manuscript Submitted for Publication]

[2] United Nations Security Council. (2023). *Midterm Report of the Panel of Experts Submitted Pursuant to Resolution 2680. S/2023/656.* https://undocs.org/S/2023/656.

[3] Barnhart, Michael. (2025). Exposing DPRK’s Cyber Syndicate and Hidden IT Workforce. DTEX.

[4] Crowe, Audrey. (2026). “Weaponizing the AI–Insider Convergence: How Threat Actors Hijack Legitimate Access Pathways”. In *Artificial Intelligence and the Security of Civilian Nuclear and Radioactive Materials, Facilities and Activities.* Ed. Sarah Case-Lackner. Springer . [Manuscript Submitted for Publication]