Overview on how to mitigate insider risks in general

Lisa De Laet/FANC and Paula Karhu/STUK

INFCIRC/908: Regional Workshop on Addressing Evolving OT Impacts for ITM and Supply Chain Security

16-18 June 2026, STUK, Vantaa, Finland

Insider threat

- Insider is
  - an individual with authorized access [to nuclear material, nuclear facilities, nuclear fuel transports or to sensitive information or sensitive information assets] who could commit or facilitate the commission of criminal or other intentional unauthorized acts with harmful consequences
- Insider has
  - access
  - authority
  - knowledge
- Insider threat can be
  - active, passive, unwitting, violent, non-violent

stuk

Insider threat mitigation

- An incident is possible when capability, opportunity and intent exist at the same time
- People are a big attack surface
- Internal attack vectors are more probable than external – still controls concentrate more on the latter (”trusted people using trusted systems”)
- ”Prevent doing the wrong thing and make it easy to do the right thing”
- Prevention, detection, response
- Graded approach

- [INFCIRC/908 International Practitioner Workshop for Insider Threat Mitigation at Nuclear & Radiological Facilities, 18-22 Sep 2023, Sandia National Laboratories, Albuquerque, NM]

stuk

Insider threat mitigation programme 1/2

- Trustworthiness assessment including background checks
  - Work history, financial, criminal, compliance…
- Controls when duties change and at the end of employment
- Fitness for duty programme
  - including health including psychological evaluation
- Behavioural observation programme, red flags
- Reporting of observations
- Self-reporting
- Physical access management
- Two-person rule
- Culture of safe environment and support
- **Finding the right people for the right jobs**

”If you see something, say something”

stuk

[INFCIRC/908 IPW for ITM at NF & RF, 18-22 Sep 2023, SNL, Albuquerque, NM]

Insider threat mitigation programme 2/2

- Technical methods
  - Contraband detection
  - Camera surveillance
  - Nuclear material accounting and control
  - Information security
    - Monitoring of networks and information systems
    - Access management, least privileges, logging
    - Malware protection, hardening of devices
    - AI methods…
    - Cyber forensics
  - Balancing with privacy regulation
- Assessment of effectiveness

ITM is multidisciplinary!

stuk

[mostly: INFCIRC/908 IPW for ITM at NF & RF, 18-22 Sep 2023, SNL, Albuquerque, NM]

Critical path

- Personal predispositions
  - medical/psychiatric conditions, previous rule violations, social network risks
- Stressors
  - personal, professional, financial
- Concerning behaviours
  - interpersonal, security, financial, personnel, social network, travel, mental health/addictions
- Bad organization responses
  - inattention, no risk assessment process, inadequate investigation, summary dismissal or other actions that escalate risk
- Harmful act
- [Eric Shaw and Laura Sellers: Application of the Critical-Path Method to Evaluate Insider Risks, Studies in Intelligence Vol 59, No. 2 (Extracts, June 2015)]

Summary: defence in depth in ITM

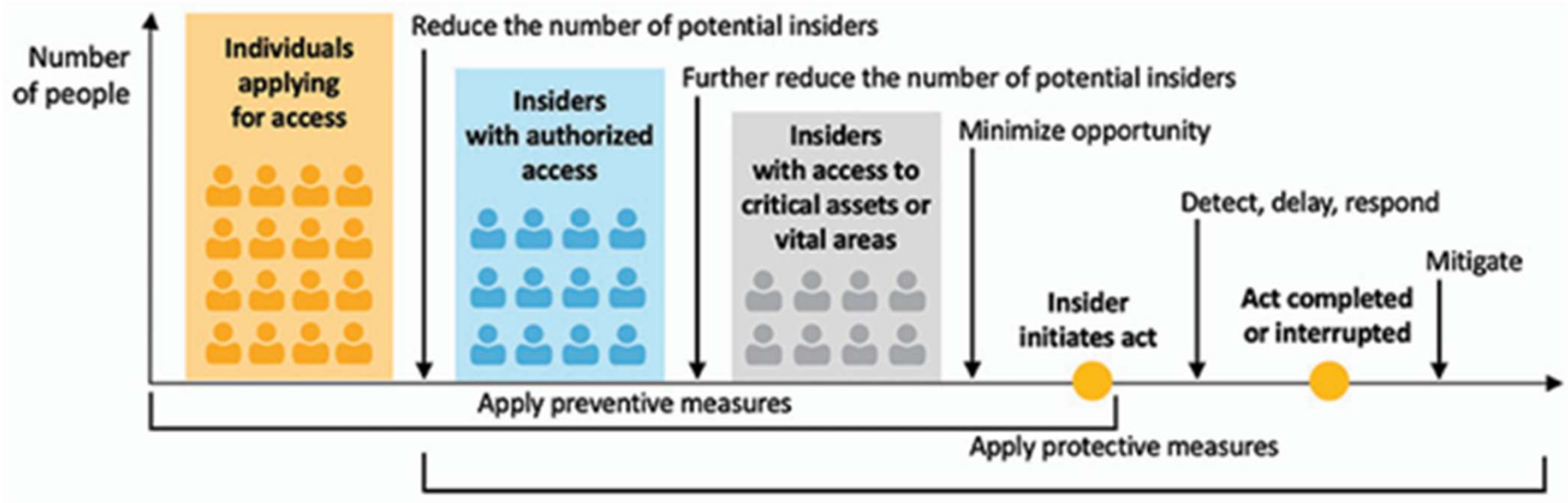


FIG. 1. Steps for using preventive and protective measures against potential insider threats.

- [NSS No. 8-G (Rev. 1) Preventive and Protective Measures Against Insider Threats, IAEA]

stuk

Preventive measures: Trustworthiness

IAEA Technical guide on Trustworthiness (NSS 51-T) & highlights from the Personnel Vetting Survey (2023)

Establishment and Implementation of a Trustworthiness Programme for Nuclear Security (NSS 51-T)

- Published January 2026
- Goal: Trustworthiness determination & monitoring of reliability and integrity
  - Principles of determination of trustworthiness
  - Roles of stakeholders (State, licensees, individuals,…)
  - Implementation of a trustworthiness program (**graded approach**)
  - Criteria for assessment and determinations
  - Maintenance of records
  - Life cycle elements
  - Protection of individuals
  - Reporting criteria
  - Audit and inspections

→ Start of a common understanding (theory)

stuk

Survey: Understanding Global Good Practices in Personnel Vetting for Nuclear Security (2023)

- Developed by members of the *Advancing INFCIRC/908 International Working Group*

Key Questions

- How does the regulator or other agency (e.g., security services) determine the reliability and trustworthiness of individuals with access to sensitive information and/or nuclear and other radioactive materials?

- Is there a legal basis for personnel vetting?

- Are there similarities or differences between vetting approaches used by Member States?

- What are the core attributes of an effective insider threat mitigation program?

stuk

→ ***Global Good Practices*** ←

Categories in the questionnaire

stuk

Survey Highlights

56% of Member States Responded

- 32 INFCIRC/908 subscribing Member States; 18 responded to the survey
- Survey responses received between February 22 and May 15, 2023

30% of Member States require

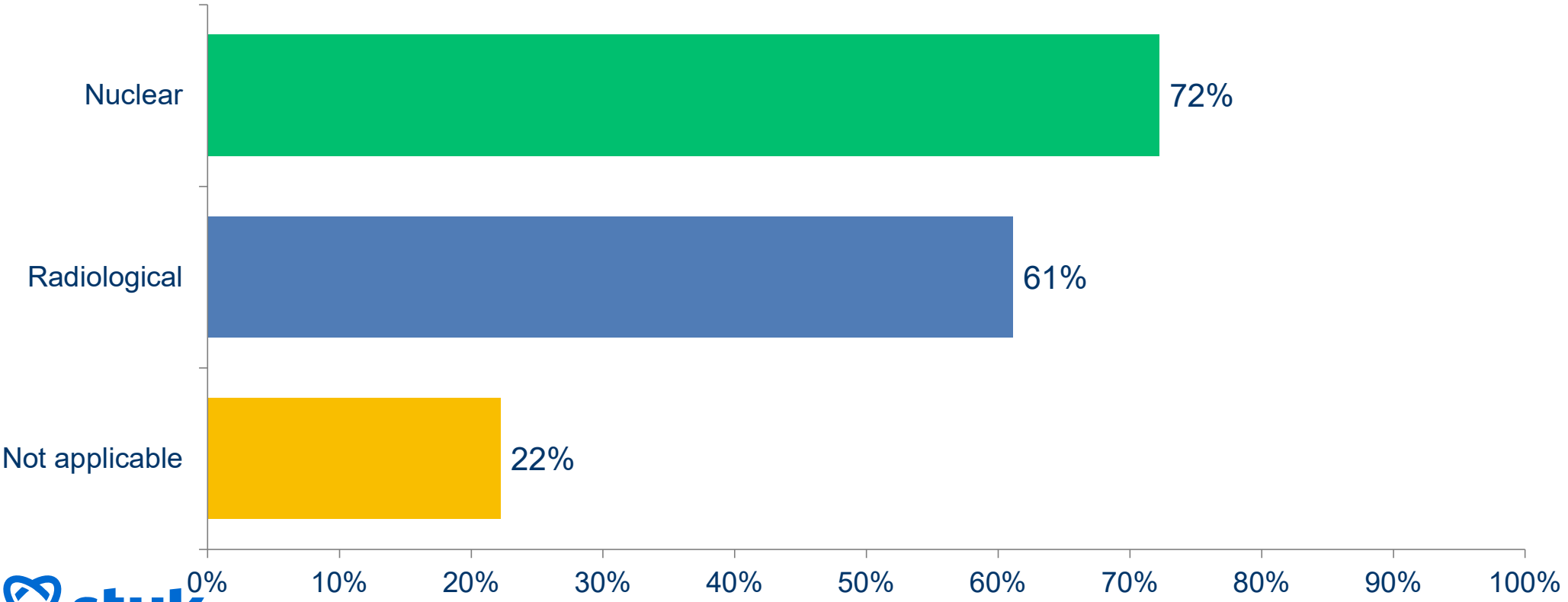
- A psychological test or consultation
- Medical test or consultation
- Mental Health evaluation

73% of Member States Prioritize Personnel Vetting

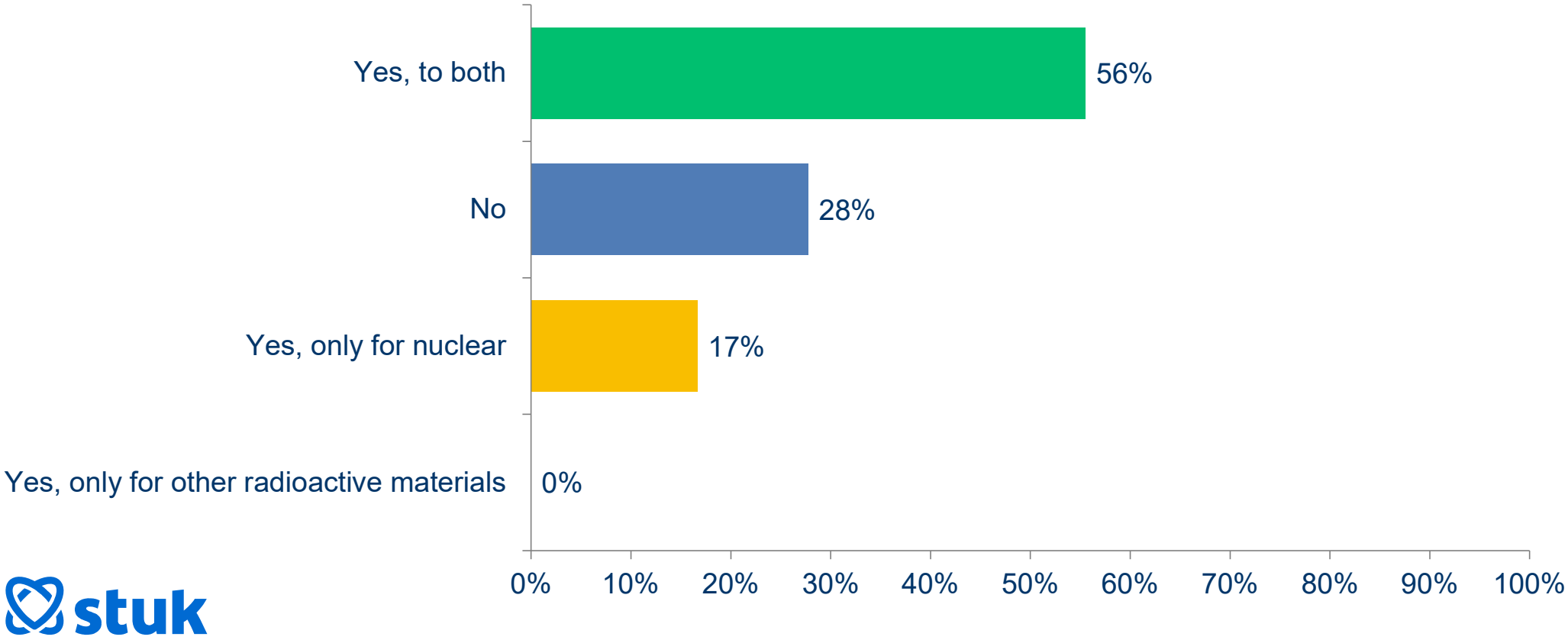
Vetting is defined as the process by which a determination of a person's trustworthiness and/or reliability is made, and which includes verifying details and characteristics of the individual.

stuk

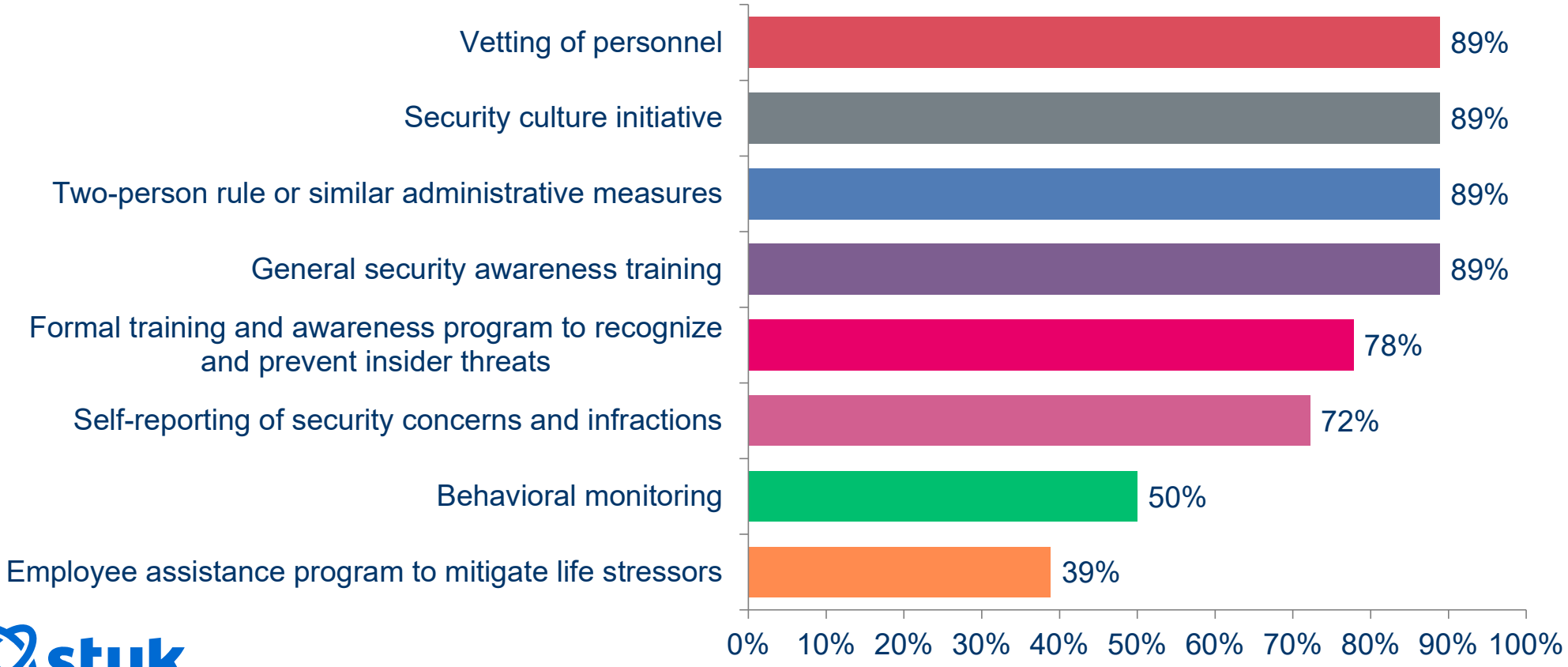
Is insider threat defined within your State's nuclear and/or radiological security regime? and/or radiological



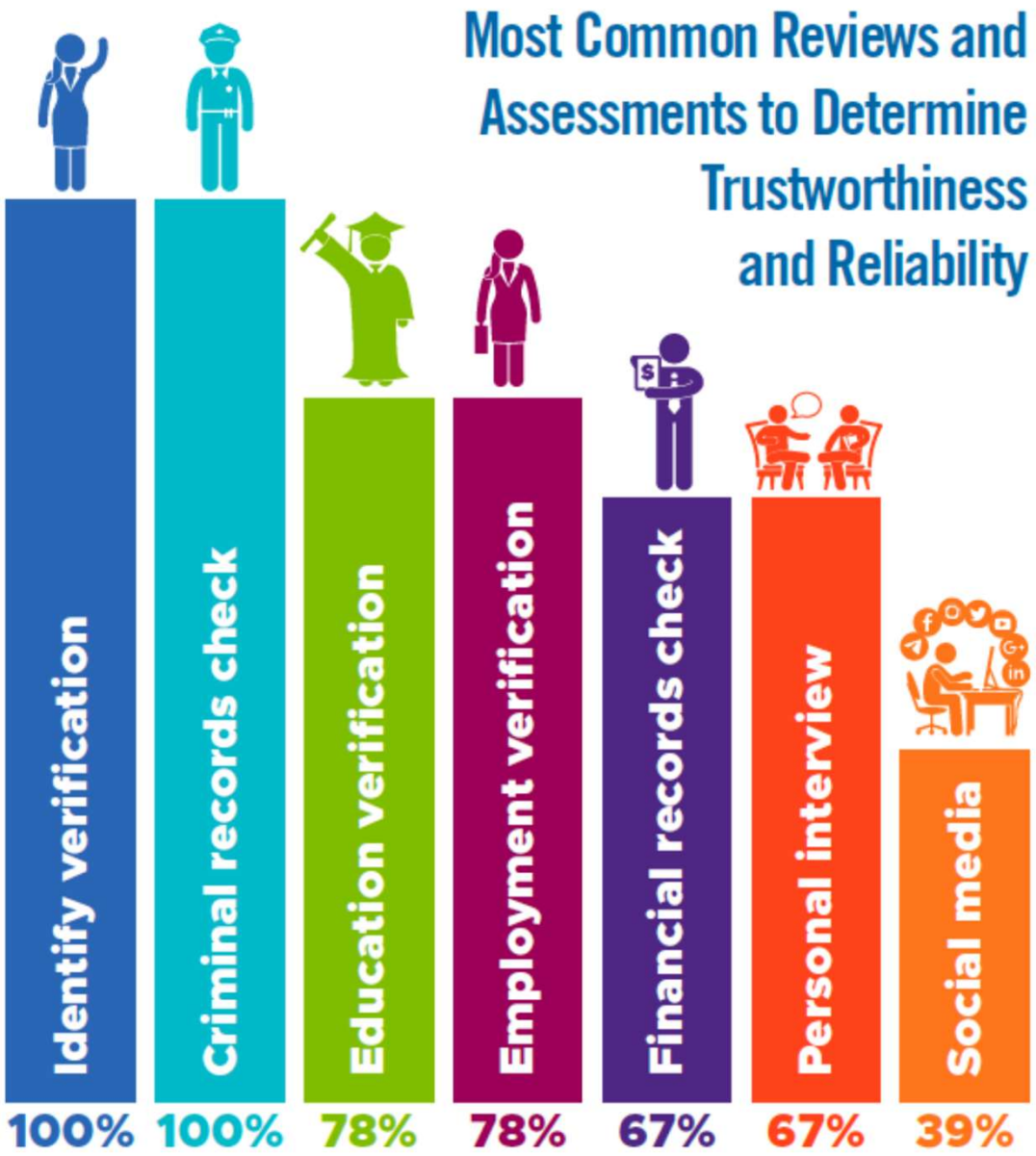
Does the State regulation, law, or policy require nuclear and/or radioactive material licensees or authorized users to have an insider threat mitigation program?



What does the State regulation, law, or policy identify as the core elements of an insider threat mitigation (ITM) program?



stuk



Top 5 Vetted Populations

1. Employees/Staff (100%)
2. Contractors & sub-contractors (75%)
3. Affiliates (e.g., student workers, researchers) (50%)
4. Vendors (50%)
5. Unescorted visitors (40%)

Similarities and Differences Between the Survey and NSS 51-T, *Establishment and Implementation of a Trustworthiness Programme in Nuclear Security*

Identified in Survey, not in NSS 51-T

- Personal Interview
- Vetting of Cohabitants
- Social Media Review
- Fingerprints or biometrics
- Mental Health Evaluation

Identified in NSS 51-T, Not in Survey

- Travel History
- Polygraph Screening

stuk

Final Thoughts

- No “one-size fits all”

- Vetting programs are influenced by social, cultural and political conditions, pandemics, …

- **88%** have published guidance on personnel vetting

- **88%** have formal information sharing agreements between agencies and organizations involved in vetting process

- **77%** of States use role-based or risk-informed approach to conduct vetting

stuk

Thank you!

Lisa.DELAET@FANC.FGOV.BE
paula.karhu@stuk.fi