Continuous Evaluation: Balancing Security & Privacy

Breakout Session

Overview

Once implemented, continuous evaluation will allow a more efficient process of vetting trusted employees in the IC , thereby mitigating insider threat concerns. However, technology, social media, and privacy concerns all pose challenges that the IC and its industry partners must address.

Summary

Comprised of Intelligence Community officials and industry experts, this panel discussed the challenges in implementing continuous evaluation; the issue of balancing personal privacy and social media; the transition to Trusted Workforce 2.0; and the potential applications of automation and machine learning.

Panelists

- **Moderator: David Buckley**, Managing Director, KPMG
- **Sharon Claridge**, Booz Allen Hamilton
- **Brian Dunbar**, Assistant Director of Security, National Counterintelligence and Security Center
- **Ben Huebner**, Office of Civil Liberties, Privacy and Transparency, ODNI
- **Tricia Stokes**, Director of Defense Vetting, DCSA

Key Takeaways:

- The government is shifting its personnel security paradigm from routine, periodic reinvestigations to continuous evaluation. Approximately 1.4 million individuals are currently enrolled in DOD's continuous evaluation program.
- Continuous evaluation implementation guidelines mandate checks in seven required data categories, including involvement with terrorism, public records checks, credit, and suspicious financial transactions.
- Automation and machine learning have the potential to improve and expedite continuous evaluation; however, industry and government must be aware of potential bias in screening and adjudication processes.
- Review of a worker's social media accounts, which could identify personal views and activities of potential concern, nevertheless raises thorny privacy issues. As the IC draws increasingly on publicly available electronic information for its continuous evaluation programs, guidelines for the review of social media will be needed.

Recommendations

- In implementing continuous evaluation across the IC, agencies should establish common standards for trust, which will facilitate reciprocal acceptance of clearances .
- Government and industry organizations must establish clear guidelines regarding the balance between the IC's security requirements and a worker's personal privacy and civil liberties.
- Agencies must seek methods to remove bias from automated review of publicly available information.

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is the leading nonpartisan, nonprofit trade association for driving public-private partnerships to advance intelligence and national security priorities. A 501(c)(6) membership organization, INSA strives to identify, develop, and promote collaborative approaches to national security challenges. INSA has more than 160 organizations in its membership and enjoys extensive participation from leaders and senior executives in the public, private, and academic sectors. Learn more at www.INSAonline.org.