STATEMENT BY

DR. RADHA IYENGAR PLUMB

DEPARTMENT OF DEFENSE
CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICER

BEFORE THE

SENATE SELECT COMMITTEE ON INTELLIGENCE

ON

# NATIONAL BACKGROUND INVESTIGATION SYSTEM AND OTHER MATTERS RELATED TO TRUSTED WORKFORCE 2.0 AND PERSONNEL VETTING

JULY 10, 2024

Chairman Warner, Vice Chairman Rubio, and distinguished members of the Committee, I appreciate the opportunity to testify before you today on the National Background Investigation Services, or NBIS, program, and our efforts to support a modern, end-to-end personnel vetting process.

As you heard from the other witnesses, the Chief Digital and Artificial Intelligence Office has partnered with our colleagues across the Department of Defense (DoD) to realign NBIS governance and development processes through the Defense Counterintelligence and Security Agency (DCSA) 90-day Recovery Plan.

In February 2024, the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) requested the Chief Digital and Artificial Intelligence Office (CDAO) and its Defense Digital Service (DDS) to perform a technical assessment of NBIS.

To formulate recommendations, we conducted a 90-day discovery initiative, in close cooperation with DCSA. During this process, the CDAO team learned about the overall problem space, user needs, as well as mission and technical requirements. We then worked with partners across DoD to ensure any proposed technology changes aligned to the full set of requirements for NBIS.

As we've seen in other enterprise-level implementations within DoD and with analogous examples in private industry, modernizing and scaling a technical capability doesn't just require a change to the underlying technologies but also a change in mindset and culture. For that reason, our recommendations highlight both the "what" (i.e., the technology) and the "how" (i.e., the people and processes).

CDAO made a number of specific recommendations to help DCSA deliver a technical NBIS solution that meets the needs of DoD and the federal government. These include:

**1. Data Architecture:** Rather than treat NBIS as a single, monolithic system, we believe the best approach going forward is to maintain a modular architecture to enable flexibility and adaptability for future changes. That modularity allows NBIS to leverage existing applications that are working well today and focus resources on addressing other components with the greatest technical risk.

To drive down technical risk, we recommend migrating to more modern and reliable compute and storage infrastructure using modern software engineering approaches. This then allows NBIS to achieve modularity more rapidly by investing in Application Program Interfaces (APIs). These essentially create common connectors between different components.

This process to connect different components will also rely on identifying and consolidating data sources, developing data standards, and deduplicating data where it exists, with the ultimate goal of having a shared data service.

**2. Build the Right Teams**: CDAO and our DDS team believe having the right people, with the right skillsets, is critical to delivering on our technical recommendations.

In particular, this includes a team developing a BI application using Trusted Workforce 2.0 as a first principle and ensuring an appropriate government and contractor workforce with technical skills, data and IP rights management, and API interface design and maintenance.

This also includes integrating product trios of product manager, user experience/research & design, and engineer, and aligning teams on products rather than features or capabilities.

**3. Adopt digital transformation best practices**: It is essential to recognize the unique challenges of conducting agile software development within the government sector. Agile methodologies, which emphasize iterative progress, flexibility, and customer collaboration, can often conflict with perdurable government processes and deep-seated culture.

This includes adopting an agile and customer-first mindset across all organizational levels to foster a cohesive, responsive, and efficient working environment. To support that, we should align requirements gathering to User-Centered Design and Agile software development within the NBIS Program Office and ensure the Authorizing Official (AO) responsible for cybersecurity follows an approach that affords iteration while maintaining compliance.

Leveraging the elevated requirements and acquisition processes, we believe these technical recommendations enable the NBIS program to significantly improve its system architecture, organizational structure, and user experience, ultimately ensuring a more secure and efficient background investigation process for DoD and the federal government.

While the path to modernizing our personnel vetting systems faces challenges, the strategic decision to build upon existing systems, combined with the expansion of technical talent and the adoption of agile methodologies, provides a robust framework for success. With these measures in place, NBIS is well-positioned to enhance the efficiency, security, and effectiveness of our personnel vetting processes, ultimately strengthening our overall national security infrastructure.

Lastly, and perhaps most important, we need to acknowledge that software delivery never reaches a discrete endpoint. Unlike hardware procurement, we should anticipate to always devote time and resources to maintaining and improving the technology. This is a mindset shift that needs to be applied to NBIS.

CDAO looks forward to continuing to work with DCSA in designing, developing, and deploying a viable, desirable, feasible, and usable NBIS program.

Thank you to the members of this Committee for your ongoing support and collaboration, and I look forward to answering your questions.