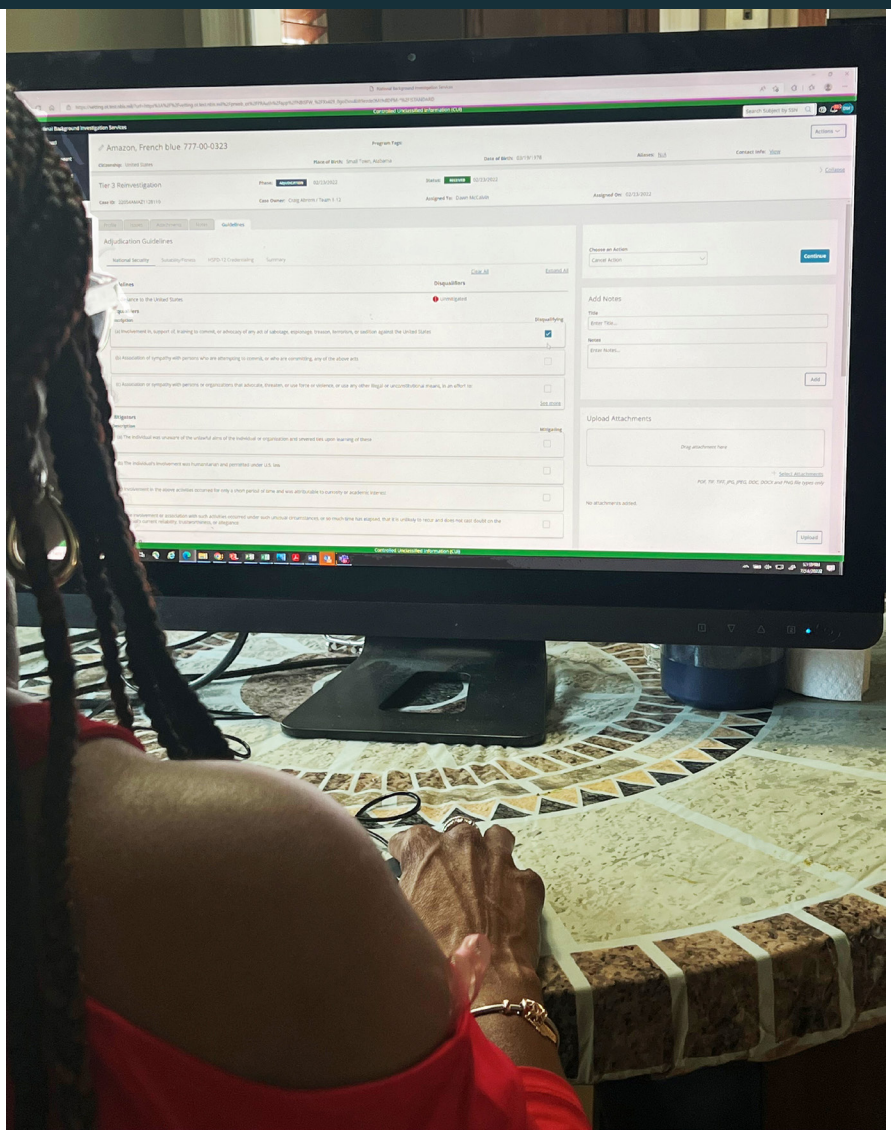
# National Background Investigation Services (NBIS)




**In FY24, the National Background Investigation Services (NBIS) Program Office conducted a comprehensive re-structure of its acquisition strategy, and changes to the overall Evaluation Strategy are expected to follow in FY25. The program employs Agile software development techniques to field and build out capabilities in support of personnel security vetting missions. DOT&E observed limited operational testing in 1QFY24, but these events were not sufficient to assess program performance.**

## SYSTEM DESCRIPTION

NBIS is a cloud-based system-of-systems that will integrate both new and legacy systems to support all tasks associated with end-to-end personnel security vetting and continuous reviews. NBIS applications are integrated in a common architecture to support data gathering, storage, and management of data associated with personnel background investigations in a secure and protected environment.

## MISSION

The Defense Counterintelligence and Security Agency (DCSA), other Federal agencies, and industry partners will use NBIS to authorize and support background investigations for new applicants as well as incumbent government, military, and contract personnel. NBIS has four operational mission areas: case initiation, adjudication, continuous vetting, and background investigation. It also has three cross-cutting support missions: service operations, metrics and reporting, and subject management. These missions allow agencies to initiate clearance requests, enable candidates to complete background investigation forms, gather public data concerning personnel applying, manage the findings of an investigation, adjudicate personnel clearances, and provide continuous vetting of cleared personnel. The system of systems also simultaneously supports and measures system performance across these functions.

## PROGRAM

NBIS transitioned to the software acquisition pathway in FY21 and is being developed using Scaled Agile Framework (SAFe) and Development Security Operations (DevSecOps) methodologies. The DCSA assumed operational control for NBIS from the Defense Information Systems Agency in October 2020 and is deploying NBIS in multiple releases of increasing capability, while building upon some legacy systems. The program has employed SAFe methodologies to rapidly develop and field capabilities in collaboration with the testers and intended customer/user base. Early releases to a limited and restricted user base supported continuous developmental testing and a cumulative validation of system and data security. In March 2022, DOT&E placed NBIS on oversight due to program size, complexity, and importance to DoD operations. DOT&E has approved an NBIS Evaluation Strategy and an online test management process for NBIS. Following a comprehensive program review in FY24, the program office has modified the service and capability delivery schedules and methods to migrate and modernize legacy systems and reduce new software production. This change required a revised Evaluation Strategy. DOT&E approved the revised Evaluation Strategy in 1QFY25.

## » MAJOR CONTRACTORS

- Peraton, Inc. – Reston, Virginia (software development)
- HII – Newport News, Virginia (big data platform)
- Copper River Information Technology, LLC – Chantilly, Virginia (systems engineering)
- GovCIO – Eatontown, New Jersey (operations support)

## TEST ADEQUACY

NBIS testing has largely focused on developmental software validation and release. Joint Interoperability Test Command (JITC) has completed multiple rounds of cyber survivability tests and began conducting the first operational assessment (OA) in FY24. DOT&E approved the NBIS Evaluation Strategy in December 2022 and approved an online test management process that makes extensive use of online planning software, in lieu of written test documents, for NBIS in July 2023, as a pilot effort with potential relevance to other Agile software developments. JITC conducted a partial OA of the case initiation mission area in 1QFY24, observed by DOT&E, but it was incomplete and not sufficient to assess program performance. JITC also conducted two cyber survivability tests in 3QFY24 and 4QFY24. Additional OA events were included in the updated Evaluation Strategy.

## PERFORMANCE

### » EFFECTIVENESS

The operational mission areas of NBIS are developing at different rates: case initiation and adjudication capabilities are both relatively mature. Continuous vetting capabilities continue to mature, and background investigations capabilities are in early development. The cross-cutting mission areas are also in varying stages of maturity at this time. The partial OA of case initiation was incomplete and therefore the effectiveness of this mission area cannot yet be fully assessed.

### » SUITABILITY

Suitability testing is ongoing, and assessments of issue tracking and resolution, training, and helpdesk support are not yet completed. The partial OA of case initiation was incomplete regarding suitability, and further development of the system monitoring and help desk capabilities is needed prior to the next OA.

### » SURVIVABILITY

Several rounds of cyber survivability testing have been conducted on NBIS and relevant connected legacy systems. Based on a 2024 assessment, the system is currently considered not survivable against a moderate threat due to a vulnerability in the DoD supporting infrastructure not under control by the NBIS program. The relevant agencies have stood up a working group to address this finding.

## RECOMMENDATIONS

DCSA and the NBIS Program Office should:

1. Continue development of the online test management process and automated test support.
2. Work with the appropriate stakeholders to address infrastructure cyber vulnerabilities to ensure NBIS is cyber-survivable.