



Pentagon, AI under scrutiny: doubts over its ability to detect liars, program scaled back

The DCSA has excluded some technologies from the current project. Earlier documents described models to analyze language and emotions.

Published on 08/10/2026

The Pentagon appears to have scaled back several projects involving the use of artificial intelligence to analyze the behavior, voice, and facial expressions of personnel undergoing security screening. New statements from the U.S. Department of Defense conflict with earlier documents and presentations that described the development of automated systems to identify potential signs of deception during interviews.

According to Defense News, the initiative is part of a multiyear program to modernize the polygraph, the instrument also used in counterintelligence screenings and security clearance

procedures.

The Pentagon rules out certain technologies from the program

The Defense Counterintelligence and Security Agency (DCSA), which is responsible for screening the reliability of personnel with access to classified information, stated that the current research and development work under the Modernizing Polygraph program does not include generative artificial intelligence systems, large language models (LLMs), facial microexpression analysis, or voice assessment systems.

However, the agency said it would continue monitoring scientific developments to assess their possible future use.

The clarification does not amount to a complete abandonment of artificial intelligence. The DCSA did not clarify whether other algorithms intended to analyze spoken and written language remain active. These had previously been developed to identify communication patterns associated with deceptive behavior.

Nevertheless, the new approach marks a significant departure from guidance provided by the Pentagon in previous months.

A \$31 million program

Modernizing personnel reliability assessment tools has been the subject of studies for several years.

Documents obtained by Defense News through public records requests show that, since at least 2019, the US Air Force, the DCSA, and several university laboratories have worked on developing artificial intelligence models for sentiment analysis and detecting possible deceptive behavior.

The program, referred to in the documents as Credibility Assessment Modernization, Polygraph+ and Polygraph Next, has a total projected budget of approximately \$31 million.

The technologies under consideration include algorithms for automated results processing, decision-support tools for investigators, contactless sensors, and thermal imaging systems

capable of detecting physiological changes potentially associated with stress.

The objective is to overcome some limitations of the traditional polygraph, which records parameters such as respiration, blood pressure, and perspiration, leaving their interpretation to a human examiner.

In July, a Pentagon official explained that artificial intelligence would enable real-time data processing, providing more standardized analysis to support investigators without replacing their judgment.

Algorithms trained using data from Reddit and Twitter

Among the elements revealed in the documents was the use of content from social networks to train certain experimental models.

A DCSA presentation describes a US Air Force project to develop deep-learning algorithms for language analysis.

In the early stages, researchers used texts collected from platforms such as Twitter and Reddit, along with linguistic resources such as WordNet, to teach the systems to recognize grammatical structures, colloquial expressions, and features of everyday communication.

Another presentation, dated May 2025, outlined an experimental system in which a digital avatar would conduct part of the interview with a security clearance candidate.

Cameras and microphones would collect images, voice, and verbal content, which would then be processed by artificial intelligence models to assess the interviewee's emotional state. A human investigator would oversee the procedure, entering the questions to be put to the candidate.

According to another document, one research objective was to achieve 75% accuracy in interpreting emotional states through natural-language processing technologies.

The DCSA, however, clarified that the university involved in designing this system is not participating in the current development phase.

The scientific community questions the reliability of the results

The main obstacle concerns an algorithm's actual ability to distinguish a false statement from a true one.

Numerous scientific studies have challenged the possibility of identifying a lie through specific features of voice, language, or facial expressions.

Stress, nervousness, or a change in behavior do not necessarily constitute evidence of deception.

According to David Markowitz, a Michigan State University professor specializing in communication analysis through artificial intelligence, there are no universally reliable diagnostic indicators for detecting a lie.

In an experiment using Google's Gemini model, Markowitz compared artificial intelligence capabilities with those of humans in identifying false statements during simulated interrogations.

The results showed performance broadly comparable to chance, with accuracy close to 50%.

The experiment also highlighted a particular concern: the artificial intelligence system was more likely than human observers to wrongly attribute deceptive behavior to the people being questioned.

The risk is that algorithms may associate the mere context of an interrogation with the likelihood that the subject is hiding something.

The risk to military careers and security clearances

The issue concerns not only technological effectiveness, but also the potential professional consequences of incorrect assessments.

In the United States, the outcome of a vetting review can affect duty assignments, promotion prospects, and access to classified information.

Attorney Mark Zaid, a specialist in national security matters, noted that a negative assessment can result in lengthy periods of suspension or restricted professional opportunities.

The introduction of artificial intelligence could add another layer of uncertainty if investigators were to assign automated results greater reliability than has actually been demonstrated.

This phenomenon, known as automation bias, is the tendency to accept the recommendations of an automated system even when there is evidence that could call them into question.

The issue is particularly sensitive in national security proceedings, where opportunities to challenge a decision may be limited.

As early as 1998, in *United States v. Scheffer*, the U.S. Supreme Court highlighted the lack of scientific consensus on the reliability of the polygraph, upholding the exclusion of its results from military courts.

Between technological innovation and human oversight

The Pentagon's review of the program highlights an issue set to become increasingly important in intelligence and counterintelligence activities.

Artificial intelligence can help process large volumes of information, identify anomalies, and analyze physiological and behavioral parameters. These capabilities, however, do not automatically demonstrate that a system can determine whether a person is lying.

The distinction is particularly important when assessments concern military personnel, intelligence officials, and personnel authorized to handle classified information.

For the time being, the Pentagon has not fully clarified which artificial intelligence components remain in the polygraph modernization program, nor whether the exclusion of voice and facial analysis technologies represents a final decision.

The central question therefore remains open: what level of scientific reliability must be demonstrated before these tools can contribute to decisions capable of affecting the careers and security clearances of military personnel?

News link: <https://www.defensenews.com/news/pentagon-congress/2026/10/05/has-the-pentagon-given-up-on-ai-polygraph-analysis-of-trustworthiness/>