



Argus Research Security Platform Beta Test Report

February 2026

Executive Summary

Under the NSF SECURE Analytics cooperative agreement, a structured six-week beta test of the Argus Research Security Platform was conducted with 58 research security, compliance, and research administration professionals representing universities, research institutes, hospital systems, and small businesses. The purpose of the beta test was to validate the operational relevance of the platform, identify requirements necessary for institutional trust and scalability, and translate participant feedback into prioritized development actions prior to broader deployment.

Core Validation: Mission Relevance

The beta test confirmed that Argus addresses a significant operational gap in research security due diligence by centralizing entity data, affiliations, publications, funding sources, and restricted-party indicators into a unified analytical workflow. Participants consistently reported that consolidating these fragmented data sources materially reduces the manual burden associated with research security reviews and improves analytical consistency. Testers used the platform to identify entities and individuals appearing on U.S. restricted party lists, assess foreign affiliations and countries of concern, evaluate publication and co-author risk, examine funding sources and research domains, and export results to support institutional documentation and decision-making. Across use cases, the conceptual alignment between Argus and day-to-day institutional research security responsibilities was clear.

Institutional Trust Thresholds

While mission relevance was validated, the beta test surfaced critical trust thresholds that must be met before institutions will operationalize the platform at enterprise scale. Participants emphasized that conceptual alignment alone is insufficient for adoption. Demonstrable data integrity, explainable risk indicators, stable system performance, and defensible documentation outputs are non-negotiable requirements. Institutional research security decisions carry regulatory, reputational, and financial implications, and even isolated inaccuracies can undermine confidence in downstream risk signals.

Data Accuracy and Entity Resolution

Data accuracy and entity resolution emerged as foundational concerns. Although testers valued Argus's ability to identify restricted entities and high-risk affiliations, they identified issues including duplicate or fragmented entity records, inconsistent handling of alternate names and transliterations, occasional misattribution of individuals to incorrect institutions, and incomplete linkage between laboratory-level entities and parent organizations. Participants made clear that confidence in the



overall system depends on reliable entity resolution, as errors at this level cascade into broader risk assessments.

Risk Flag Persistence and Explainability

Risk flag persistence and explainability were identified as essential for institutional defensibility. Integrated restricted party list screening significantly accelerated due diligence workflows; however, participants noted that risk indicators were not always persistent across entity and drill-down views, that list memberships were sometimes incompletely displayed, and that explanations of why a particular entity or individual was flagged were limited. Testers further emphasized the need to clearly distinguish between direct restrictions and affiliation-based or derivative risk. Institutions require transparent, source-attributed indicators that specify the originating list and the rationale for the designation in order to support defensible decision-making.

Enterprise-Scale Workflow and Reporting

Participants highlighted enterprise-scale workflow considerations, including the need for advanced search and filtering capabilities, continuity across cases, and reliable export and reporting functions. Documentation generated by the platform must be accurate, complete, and audit-ready, as institutions rely on these outputs to demonstrate compliance and due diligence. In addition, overall platform stability, performance consistency, and appropriate access controls were identified as prerequisites for adoption in regulated institutional environments.

Development Response and Next Build Cycle

Feedback from the beta test has been consolidated into structured development workstreams that are shaping the next build cycle. Priority efforts include strengthening entity resolution logic, ensuring persistence and transparency of risk indicators, expanding enterprise search and filtering functionality, stabilizing reporting and export features, and improving overall system reliability and access control mechanisms. The beta phase therefore served not only as validation of conceptual fit but also as a mechanism for defining the operational standards required for broader institutional deployment.

Strategic Conclusion

The beta test validated that Argus aligns directly with institutional research security needs and meaningfully reduces the inefficiencies associated with fragmented due diligence processes. However, institutional adoption will depend on the platform's ability to meet clearly defined thresholds of accuracy, explainability, scalability, and defensibility. The strategic opportunity is evident, and the path forward is defined by the translation of validated mission relevance into demonstrable institutional trust.