Q2.

FISSEA Innovator of the Year Nomination Form

Submission Deadline: March 27, 2026, at 11:59 PM ET

Q3.

Person making this nomination:

Name	George Bailey
Organization	Purdue University
Position or Title	Director, cyberTAP
Email Address	

Q4.

Person being nominated:

Name of Nominee	Jordan Scott
Nominee's Employing Organization	Code Talkers Engineering
Nominee's Position and/or Title	Principal Investigator, DARPA STTR Phase 1 COPE Project
Nominee's Email Address	
Nominee's Phone Number	

Q5.

Justification for nomination:

Include a brief description of the impact the individual has had on the awareness and training program within his or her organization.

Examples include: creating an innovative awareness program training and that strengthens the cybersecurity of a federal department or agency, providing frequent status updates to senior management about awareness and training outcomes that reduce enterprise risks, and leading an awareness- and training-related program or project with limited resources.

Direct Federal Benefit As a DARPA STTR Phase 1 project, COPE directly supports Department of Defense objectives in developing a skilled cybersecurity workforce for space systems—a critical national security priority. The Space ISSO pilot program addressed immediate training needs for positions essential to protecting space assets and maintaining critical space infrastructure's Confidentiality, Integrity, and Availability. The framework's rapid curriculum development capability is particularly valuable for federal agencies facing: ▪ Quickly evolving threat landscapes requiring immediate training updates ▪ Specialized roles with limited existing training resources ▪ Budget constraints that make traditional curriculum development prohibitive ▪ Need for consistent, standardized training across distributed teams

Q6. Do you have documents to include with your submission?

FISSEA training contest nominiation.pdf
109.5KB
application/pdf

To Whom It May Concern,

Mr. Jordan Scott's groundbreaking work as Principal Investigator of the DARPA STTR Phase 1 COPE (Cybersecurity Operations Professional Education) project represents a transformative advancement in cybersecurity training methodology. His development of a systematic framework integrating Generative AI with established instructional design principles has revolutionized how specialized cybersecurity training can be rapidly developed and deployed to address critical workforce gaps in the space industry and beyond.

Major Accomplishments and Innovations

Revolutionary Training Framework Development

Mr. Scott created the first systematic framework that integrates Retrieval Augmented Generation (RAG) with the ADDIE instructional design model specifically for cybersecurity education. This innovation directly addresses one of the most pressing challenges in federal cybersecurity workforce development: the inability of traditional curriculum development to keep pace with rapidly evolving threats and specialized domain requirements. While traditional approaches require 6-12 months and large expert teams costing up to $50,371 per hour of advanced learning modules, Mr. Scott's framework generates comprehensive, pedagogically sound training materials within hours.

Addressing Critical Space Cybersecurity Workforce Gaps

Through comprehensive market research involving 33 industry professionals, Mr. Scott identified critical gaps in existing cybersecurity training frameworks, particularly for specialized positions like Space Information Systems Security Officers (ISSOs). His research revealed that 82% of employers emphasized soft skills as equally important to technical skills, and 67% required holistic system understanding beyond traditional cybersecurity domains—requirements that existing frameworks like NICE did not adequately address.

In response, Mr. Scott systematically extended the NICE Framework beyond its original 2,200+ cybersecurity KSTs by generating over 500 additional domain-specific Knowledge, Skills, and Tasks (KSTs) across six critical areas: Space Operations, Soft Skills, Systems Engineering, Industrial Control Systems, Agile Methodologies, and Intelligence Operations. This expansion provides a replicable methodology for adapting cybersecurity training to any rapidly evolving technical domain.

The Inverted Security Risk Taxonomy

One of Mr. Scott's most innovative theoretical contributions is the development of the Inverted Security Risk Taxonomy, which challenges traditional learning frameworks by prioritizing training time based on incident impact rather than probability. This approach recognizes that while high-likelihood cybersecurity events require only basic knowledge, rare but catastrophic events demand deep expertise and complex problem-solving capabilities. This framework provides a systematic approach for resource allocation in cybersecurity training that better prepares professionals for high-impact scenarios—particularly relevant for critical infrastructure protection.

Comprehensive Curriculum Generation Capabilities

Mr. Scott's framework demonstrates unprecedented efficiency in generating diverse, high-quality educational materials:

- 500+ domain-specific KSTs mapped to job requirements
- Modular lecture materials across Foundation, Intermediate, and Expert competency levels
- 886 tagged assessment questions in GIFT format for direct LMS integration
- Interactive gamified exercises incorporating space simulations (KerbalEDU) and cybersecurity challenges (HackTheBox)
- User story-based exercises enabling agile, self-directed learning

All content undergoes multi-stage validation including subject matter expert review, educational design assessment, and industry stakeholder confirmation—ensuring both technical accuracy and pedagogical effectiveness.

Impact on the Public Sector

Direct Federal Benefit

As a DARPA STTR Phase 1 project, COPE directly supports Department of Defense objectives in developing a skilled cybersecurity workforce for space systems—a critical national security priority. The Space ISSO pilot program addressed immediate training needs for positions essential to protecting space assets and maintaining critical space infrastructure's Confidentiality, Integrity, and Availability.

The framework's rapid curriculum development capability is particularly valuable for federal agencies facing:

- Quickly evolving threat landscapes requiring immediate training updates

- Specialized roles with limited existing training resources
- Budget constraints that make traditional curriculum development prohibitive
- Need for consistent, standardized training across distributed teams

Measurable Learning Outcomes

Pilot implementation with Space ISSO trainees demonstrated substantial educational effectiveness:

- Test scores improved from 73.9% to 92.1%
- Self-reported capability ratings increased from "low-moderate" to "high" across all competency areas
- Students generated real-world deliverables including automated satellite launch sequences with cyber attack simulations
- Participants reported learning more "with project and game-oriented learning than in years of traditional methods"

Broader Public Sector Applications

The framework's systematic approach extends beyond space cybersecurity to any technical field requiring current, industry-aligned training. Mr. Scott's methodology for translating industry stakeholder requirements directly into educational materials provides federal agencies with a replicable process for:

- Rapidly developing training for emerging technologies
- Adapting existing programs to new regulatory requirements
- Creating specialized training for mission-critical roles
- Maintaining training currency in fast-evolving domains

The research findings have already influenced approaches to general cyber awareness training, with planned implementation for broader federal workforce development this summer.

Scope and Breadth of Accomplishments

Industry Validation and Collaboration

Mr. Scott's work demonstrates exceptional collaboration across government, industry, and academia. The COPE project involved partnerships with Purdue University's cyberTAP Lab

and SpaceISAC, ensuring the framework addressed real-world operational requirements. His systematic interview process with 33 industry professionals provided empirical foundation for curriculum design—an approach that ensures federal training investments align with actual workforce needs.

Industry stakeholder feedback directly informed framework development, with employers providing iterative input through agile sprint reviews. This collaborative approach resulted in immediate practical impact, with students receiving job offers during training demonstrations and employers implementing security improvements based on student projects.

Research Contribution and Dissemination

Mr. Scott's research has been accepted for publication in peer-reviewed IEEE conferences (ISNCC 2025), ensuring his methodological innovations are available to the broader cybersecurity education community. His work addresses critical gaps identified in systematic reviews of cybersecurity training, particularly the need for:

- Content appropriateness for specific user groups
- Hands-on activities for practical skill development
- Cost-effective, scalable training solutions
- Alignment with established frameworks while incorporating innovation

Scalability and Sustainability

The framework's architecture supports sustainable workforce development through:

- Automated content generation processes reducing long-term maintenance costs
- Modular design enabling targeted updates without complete redesign
- Quality assurance mechanisms ensuring consistent educational standards
- Extensibility to other technical domains beyond initial space focus

Individual Contribution and Leadership

As Principal Investigator of the DARPA STTR Phase 1 COPE project, Mr. Scott provided visionary leadership in conceptualizing, designing, and implementing this innovative training framework. While the project involved partnership with Purdue University's cyberTAP Lab (George Bailey) and SpaceISAC, Mr. Scott's distinct contributions include:

Primary Responsibilities:

- Conceptual design of the RAG-ADDIE integration framework
- Development of the Inverted Security Risk Taxonomy
- Design and execution of the 33-person industry requirements study
- Creation of systematic prompt engineering processes for GenAI content generation
- Development of multi-stage validation methodologies
- Framework implementation and Space ISSO pilot program execution
- Research methodology design and academic dissemination

Distinguished Leadership:

- Secured DARPA funding through competitive STTR Phase 1 proposal process
- Coordinated cross-institutional collaboration between UCCS, Purdue, and SpaceISAC
- Engaged industry stakeholders through NSF I-Corps Hub: West Region programs
- Developed novel pedagogical approaches combining agile learning, gamification, and simulation-based education
- Authored primary research publications documenting framework and outcomes

Mr. Scott's work represents the integration of multiple disciplines—cybersecurity, instructional design, artificial intelligence, space systems, and workforce development—into a cohesive, evidence-based training methodology. His ability to translate complex technical concepts into accessible, engaging educational experiences distinguishes this work from traditional academic research.

Originality and Uniqueness

Addressing Unmet Needs

Prior to Mr. Scott's work, no systematic framework existed for leveraging Generative AI in specialized cybersecurity training while maintaining pedagogical rigor and quality assurance. Existing AI educational tools focused on general-purpose applications, lacking comprehensive approaches that integrate:

- Industry requirements analysis
- Established instructional design principles (ADDIE)
- Domain-specific competency frameworks (NICE KSTs)

- Multi-stage validation processes
- Quality controls addressing AI hallucination concerns

Novel Methodological Contributions

Mr. Scott's framework introduces several first-in-field innovations:

1. **Requirements-Driven AI Curriculum Development:** Direct translation of job descriptions and stakeholder interviews into structured educational content through systematic prompt engineering
2. **RAG-Enhanced Educational Content Generation:** Application of Retrieval Augmented Generation specifically for cybersecurity training, significantly reducing hallucinations while maintaining rapid development
3. **Inverted Security Risk Taxonomy:** Theoretical framework prioritizing training investment based on incident impact rather than probability
4. **Agile Learning Integration:** Adaptation of software development methodologies to enable dynamic, learner-centric curriculum that responds to stakeholder feedback in sprint cycles
5. **Multi-Domain KST Extension:** Systematic process for expanding established frameworks (NICE) with domain-specific competencies validated through industry research

Future Impact and Sustainability

The COPE framework's impact extends beyond immediate training outcomes. Mr. Scott has established:

- A replicable methodology applicable to other critical infrastructure domains
- An evidence-based approach to GenAI educational tool evaluation
- A model for industry-academia-government collaboration in workforce development
- Foundation for continuous curriculum improvement through data-driven assessment

Planned summer implementation for general cyber awareness training demonstrates the framework's practical scalability beyond specialized Space ISSO applications. This broader deployment will benefit federal workforce development efforts across multiple agencies and roles.

Conclusion

Mr. Jordan Scott's innovative work as Principal Investigator of the DARPA STTR Phase 1 COPE project represents exactly the type of transformative contribution the FISSEA Innovator of the Year Award seeks to recognize. His systematic framework for GenAI-powered curriculum development addresses critical federal cybersecurity workforce needs while establishing methodological foundations that benefit the entire public sector.

By reducing curriculum development time from months to hours, extending established frameworks with domain-specific competencies, introducing novel pedagogical approaches, and demonstrating measurable educational effectiveness, Mr. Scott has created a sustainable solution to one of the most pressing challenges in federal cybersecurity: developing specialized training that keeps pace with evolving threats and requirements.

His work directly supports national security objectives in space systems protection while providing a replicable methodology applicable to any rapidly evolving technical domain requiring specialized workforce development. The originality, scope, and demonstrated impact of Mr. Scott's contributions make him an exceptionally worthy candidate for this distinguished recognition.

Respectfully,