EAGER: NAIRR Pilot Expansion: FA1: AI Horizon: Forecasting Cybersecurity Workforce Evolution and Adaptive Skill Development

Overview

The integration of AI into cybersecurity represents a fundamental transformation occurring at unprecedented speed. AI Horizon addresses the critical gap between rapid technological evolution and educational adaptation through a novel forecasting framework. This high-risk, high-reward initiative ($300,000 over two years) will predict which cybersecurity tasks will be augmented by AI, replaced by AI, or remain human-driven, enabling educators to adapt curriculum with unprecedented agility.

California State University, San Bernardino will implement this project through: (1) a Forecasting Committee identifying emerging AI-driven changes in cybersecurity workforce needs; (2) a Program Committee translating forecasts into educational strategies; and (3) partnership with Redwood Consulting for rigorous assessment. Workshops at major events (CAE Symposium, CYAD, SFS Job Fair) will reach ~1,000 academics and ~1,000 students annually, with sustainability ensured through curriculum repositories and an eventual self-sustaining conference model.

Intellectual Merit

AI Horizon advances knowledge through: (1) a data-driven forecasting framework that systematically maps AI's transformation of cybersecurity domains; (2) a novel three-committee implementation model that rapidly translates workforce insights into educational strategies; (3) innovative mechanisms for integrating NAIRR resources into cybersecurity education; and (4) advanced methodologies measuring the effectiveness of rapid curriculum adaptation. This approach represents a radical departure from traditional educational practices by compressing adaptation cycles from years to weeks.

Broader Impacts

The project strengthens national security by accelerating AI integration into cybersecurity education, creating more robust defense capabilities. It drives educational transformation by providing scalable models for rapid curriculum adaptation across 470 CAE institutions. By aligning education with emerging workplace requirements, it improves job placement outcomes and career readiness. Through effective guidance on NAIRR resource utilization, AI Horizon maximizes the impact of national AI investments on cybersecurity research and education.

This transformative approach bridges the growing gap between traditional cybersecurity education and the AI-enhanced workplace, addressing a critical national security imperative that no existing NSF program currently targets. By combining rigorous workforce forecasting with immediate classroom implementation, AI Horizon will help ensure that U.S. cybersecurity education keeps pace with technological advancement, maintaining our nation's security in an increasingly AI-driven world.

California State University, San Bernardino

EAGER: NAIRR Pilot Expansion: FA1: AI Horizon: Forecasting Cybersecurity Workforce Evolution and Adaptive Skill Development

Project Summary

AI Horizon represents a high-risk, high-reward initiative to forecast the rapidly evolving intersection of artificial intelligence and cybersecurity workforce needs. This exploratory project will establish methodologies for predicting which cybersecurity skills will be augmented, replaced, or remain human-driven in the near future, enabling educators to adapt curriculum at unprecedented speed. By leveraging NAIRR pilot resources, AI Horizon will create a direct connection between emerging AI capabilities, cybersecurity research needs, and educational practices—addressing a critical national security imperative that no existing NSF program currently targets. This transformative approach combines rigorous workforce forecasting with immediate classroom implementation, bridging the growing gap between traditional cybersecurity education and the AI-enhanced workplace. Budget: $300,000 ($150,000/year for two years).

A. Statement of Need and EAGER Appropriateness

Why This Work is Appropriate for EAGER Funding

This project represents exactly the type of "high risk-high payoff" exploration that EAGER is designed to support for three critical reasons:

1. **Unprecedented Forecasting Challenge**: This project attempts to predict the trajectory of two rapidly evolving fields simultaneously—artificial intelligence and cybersecurity. The AI landscape transforms weekly with new models, capabilities, and applications emerging at a pace that makes traditional research approaches inadequate. Forecasting in this environment is inherently high-risk, as demonstrated by previous predictions about AI's impact on coding careers. Incorrect predictions could misdirect educational resources and student career paths; however, accurate forecasting would provide invaluable guidance for curriculum development and workforce preparation that could save years of misdirected effort.
2. **Radically Different Approach**: AI Horizon introduces a fundamentally new approach to cybersecurity education by creating a continuous feedback loop between industry transformation and classroom implementation. Unlike traditional curriculum development processes that operate on multi-year timelines, our approach compresses this cycle to months or even weeks—a radical departure from established educational practices that challenges fundamental assumptions about how cybersecurity education should adapt to technological change.
3. **Novel Interdisciplinary Perspective**: This work integrates methodologies from workforce development, educational research, AI implementation, and cybersecurity operations in ways no existing NSF program currently addresses. By bringing together experts from across these domains, we create unique interdisciplinary insights that wouldn't emerge through traditional siloed approaches.

This project does not fit existing NSF programs because it operates at the intersection of workforce forecasting, educational innovation, and cybersecurity research—each traditionally funded through separate mechanisms. The urgency of the need, the exploratory nature of forecasting, and the potential for transformative impact on national security make EAGER the appropriate vehicle for this work.

The Need for AI Horizon

The integration of artificial intelligence into cybersecurity operations represents more than an incremental advance in technology—it marks a fundamental transformation of how cybersecurity work is performed. This transformation is occurring at an unprecedented pace, with AI systems increasingly capable of augmenting or entirely replacing traditional cybersecurity tasks.

NAIRR pilot resources present an opportunity to accelerate research and education in this rapidly evolving domain. However, the mere availability of these resources is insufficient—researchers and educators need immediate, practical guidance on how to integrate these powerful tools into their work. In research, conducting AI experiments can be cost-prohibitive as GPUs, compute time, and other resources quickly become expensive. Having access to and learning how to use NAIRR resources is a matter of national security, as adversaries are already deploying AI to attack and penetrate networks.

In education, traditional approaches to curriculum development, which often span years from conception to classroom implementation, are no longer viable in the rapidly evolving AI landscape. By the time a textbook is published or a new course is approved through standard academic channels, the tools and techniques it covers may already be obsolete, leaving cybersecurity students at risk of graduating with skills misaligned to workplace requirements. This gap between AI's evolution and classroom content requires immediate attention—we cannot afford to wait even one traditional academic cycle to integrate these transformative tools into our educational programs.

B. Project Objectives and Activities

To address these critical needs, CSUSB proposes to establish the AI Horizon project with the following objectives:

1. **AI Transformation in Cybersecurity**: Project one academic year ahead to identify cybersecurity tasks that will be replaced by AI, augmented by AI, or remain primarily human-driven.
2. **Knowledge Dissemination**: Present workshops at established events, conduct online training, and engage with researchers and educators on these expected changes.
3. **NAIRR Resource Utilization**: Guide participants in using NAIRR resources to further research and prepare students for projected future workforce needs.
4. **Classroom Implementation**: Deliver actionable strategies for immediate integration of AI tools in cybersecurity education.

Workshops and Events

Workshops will be conducted at several high-impact events throughout the year:

- **CAE Symposium** (April 2025): Announcement of AI Horizon formation and introductory workshop on NAIRR resources. The CAE symposium reaches approximately 600 educators and researchers from over 450 CAE schools annually.
- **Cybersecurity Across Disciplines (CYAD)** (June 2025): Committee formation announcements, NAIRR resource workshops, and preliminary findings dissemination.
- **CAE Research Symposium** (October 2025): NAIRR resource workshops and initial findings from the Forecasting Committee.
- **Scholarship for Service Job Fair** (January 2026): Targeted workshops for approximately 1,000 students and 70 researchers. The team will also conduct interviews and surveys with hiring

personnel to gather insights on: a) skillsets they hoped to see but did not find in current candidates, b) anticipated skill requirements for the coming year, and c) work roles likely to be phased out.

The same sequence of events will be repeated in 2026-2027. Additionally, at least three online workshops will be conducted and recorded to maximize reach and impact.

How AI Horizon Differs from Professional Meetings

AI Horizon differs fundamentally from traditional professional meetings through its:

- Research-driven content development combining industry interviews, focus groups, and workforce analysis
- Multi-phase engagement with employers to track AI's impact on cybersecurity work
- Direct integration of NAIRR resources into classroom applications
- Connection between current workforce needs and educational adaptation
- Comprehensive evaluation strategy spanning from pre-conference research through post-implementation assessment
- Rapid dissemination of actionable strategies for curriculum updates across the CAE community
- Creation of a feedback loop between employers and educators

C. Organizational Structure

AI Horizon will operate through three specialized committees:

Forecasting Committee

This 5-7 person committee will conduct intensive analysis of emerging technologies and industry adoption patterns to identify which human-performed cybersecurity tasks are being augmented or replaced by AI systems, and which new roles are emerging. By maintaining close connections with organizations implementing AI solutions, the committee will create a practical framework of essential skills and knowledge for an AI-enhanced workplace. Members will include representatives from industry, government, and academia.

Program Committee

This 4-7 person committee will translate the Forecasting Committee's findings into practical conference elements enabling rapid adoption of AI tools in cybersecurity education. They will determine necessary presentations and workshops, gather and post resources, and demonstrate practical methods for integrating AI tools into cybersecurity curricula. Working directly with NAIRR resource providers, the committee will identify AI tools and platforms to showcase, along with streamlined approaches for educator adoption (e.g., quick-start guides and templates).

Research and Assessment

Redwood Consulting Collective will develop and deploy instruments to gather baseline data about current AI integration in cybersecurity education. At various events, they will collect quantitative and qualitative data about educator engagement with NAIRR resources, implementation plans, and anticipated

challenges. In Year 2, assessment will track actual resource adoption rates, document integration challenges and solutions, and evaluate impacts on educators' perspectives and student learning outcomes.

Leadership and Confirmed Members

- **Principal Investigator and AI Horizon Chair**: Vincent Nestler, PhD, Professor of Information and Decision Science at California State University, San Bernardino, and Director of CSUSB's Center for Cyber and AI.

Confirmed Members:

- Zoe Fowler, PhD, Principal Researcher, Career Preparation National Center
- Matthew Isnor, Branch Chief for Cyber Workforce Development, U.S. Department of Defense
- Sidd Kaza, PhD, Associate Provost for Research and Dean of Graduate Studies, Towson University
- Blair Taylor, DSc, Director of the Center for Interdisciplinary and Innovation Cybersecurity, Towson University
- Anastacia Webster, Cyber Development Lead, CISA

Additional Committee Members (pending confirmation) will be drawn from:

- CAE Symposium organizing committee
- CyberCorps® Scholarship for Service (SFS) Job Fair leadership
- NAIRR Pilot program leadership
- Academic institutions from diverse geographic areas and demographics
- Industry partners actively implementing AI in cybersecurity operations

Final committee composition will be confirmed upon award notification to ensure organizational representation and member availability.

D. Results Dissemination and Impact

AI Horizon is structured as a continuously evolving initiative. As the Forecasting Committee identifies important areas of change, the Program Committee will adapt to new information and schedule workshops to address emerging needs.

Digital Platform and Resource Sharing

A dedicated website will be created to publish information as it becomes available. This platform will evolve from an initial repository of workforce assessments to a dynamic implementation hub featuring:

- Curated quick-start guides for NAIRR resources addressing employer-identified needs
- Implementation case studies and classroom-ready materials
- Video demonstrations of AI integration in cybersecurity education
- Actionable implementation guides emphasizing immediate application

All materials will be designed to help educators begin using NAIRR resources within days rather than months.

Competition Integration

National competitions provide a powerful avenue for disseminating insights about AI-enhanced cybersecurity work roles. By partnering with established competitions like the CAE Cybergames, Collegiate Cyber Defense Competitions, and National Cyber League, we can embed findings about AI transformation directly into competitive scenarios that engage both students and educators.

Community Engagement

Regular updates through CAE Community channels will keep the broader cybersecurity education community informed of progress and findings. Monthly virtual meetings will provide opportunities for participants to share experiences and solutions. Additionally, detailed quarterly reports will be provided to NSF, including comprehensive assessment data, implementation analytics, and impact measurements.

Assessment and Evaluation

In collaboration with Redwood Consulting Collective, we will implement a comprehensive assessment strategy tracking multiple dimensions of impact:

- Successful implementation in courses
- Student engagement with AI tools
- Development of employer-identified critical skills
- Time from introduction to classroom implementation
- Impact on student job placement outcomes

To measure impact and validate workforce predictions, we will attend the January 2027 SFS Job Fair for follow-up assessment. This evaluation will help understand how accurately we predicted AI's transformation of cybersecurity work, how effectively AI Horizon events trained educators for these transformations, and how well the NAIRR integration strategies prepared students for these changes.

E. Recruitment and Support

Attendee Recruitment

We will use multiple communication channels reaching the 470 member schools in the CAE Community to recruit attendees. This community includes two- and four-year institutions with varying enrollments across 49 states in urban, suburban, and rural areas. All facilities will be fully accessible to those with disabilities.

To support broad participation, we will provide:

- Clear information about travel and accommodation options
- Guidance on accessing institutional support for attendance
- Flexible participation options for those with scheduling constraints
- Mentoring connections for new implementers
- Ongoing support for NAIRR resource adoption
- Information about childcare options

Scaling Strategy

AI Horizon is strategically designed for both immediate impact and future growth. Our initial target is approximately 1,000 academics/researchers and 1,000 students entering the federal workforce in Year 1, with similar or greater numbers in Year 2. If successful, this initiative could evolve into a full-scale annual conference dedicated to helping educators prepare for current and future workforce needs.

Based on initial interest and the accelerating pace of AI adoption in cybersecurity, future iterations could include:

- Small regional symposia focused on specific institutional contexts
- Advanced implementation workshops for experienced adopters
- Specialized tracks for different educational approaches
- Extended virtual programming for broader reach
- Enhanced support for cross-institutional collaboration

F. Long-Term Sustainability

AI Horizon is designed with sustainability beyond the two-year funding period in mind:

1. **Resource Repository**: All curriculum developed with NAIRR resources will be posted on the AI Horizon website and contributed to clark.center, a repository for cybersecurity curriculum run by Sidd Kaza and Blair Taylor, ensuring continued access and relevance.
2. **Establishment of a Working Group**: A permanent working group will be formed to continue the project's mission beyond the funding period, maintaining the connection between industry needs and educational practices.
3. **Self-Sustaining Conference Model**: If successful, AI Horizon will transition to a self-sustaining conference model, charging modest attendance fees to cover operational costs while continuing to provide valuable insights into workforce trends.
4. **Integration with Existing Communities**: By embedding AI Horizon's methodologies and findings within established communities like the CAE and SFS programs, the impact will continue to ripple through cybersecurity education long after the funding period ends.

G. Intellectual Merit

The project's intellectual merit stems from several key innovations:

1. **Data-Driven Forecasting Framework**: We are developing a sophisticated framework for identifying and disseminating emerging AI capabilities in cybersecurity, combining real-time tracking of AI's impact on work roles with intelligence gathered from employers and industry leaders.
2. **Novel Three-Committee Implementation Model**: Our implementation approach represents a significant advance in educational adaptation methodology, beginning with comprehensive workforce research that rapidly translates findings into actionable educational strategies.
3. **NAIRR Integration Mechanisms**: The project establishes innovative mechanisms for integrating NAIRR resources into cybersecurity education through streamlined adoption pathways and rapid implementation templates.
4. **Advanced Assessment Methodologies**: We are developing methodologies that measure the effectiveness of rapid curriculum adaptation, tracking not only educational outcomes but also implementation speed and workforce alignment.

H. Broader Impacts

AI Horizon's broader impacts extend across multiple dimensions of cybersecurity education and workforce development:

1. **Enhanced National Security**: By accelerating the integration of AI capabilities into cybersecurity education, we strengthen our nation's ability to defend against evolving cyber threats.
2. **Educational Transformation**: The project drives transformation by creating scalable models for rapid curriculum adaptation across the CAE community's 470 member institutions.
3. **Workforce Development**: By aligning cybersecurity education with emerging workplace requirements, we improve job placement outcomes and career readiness for students entering the cybersecurity field.
4. **Resource Optimization**: Through effective guidance on NAIRR resource utilization, we maximize the impact of these valuable national assets on cybersecurity research and education.

I. Budget

The requested budget is $300,000 over two years (approximately $150,000 per year) to support committee operations, workshop development and delivery, assessment activities, and digital platform creation and maintenance.

This project represents a unique opportunity to transform how cybersecurity education responds to the AI revolution. By creating a systematic approach to forecasting and adapting to AI's impact on cybersecurity work, AI Horizon will help ensure that U.S. cybersecurity research and education keeps pace with technological advancement, maintaining our nation's security and competitive edge in an increasingly AI-driven world.

G. Results from Prior NSF Support

PI: Tony Coulson; Co-PI: Dr. Vincent Nestler

(a) NSF Award ID: 2043237, $3.9 million, August 1, 2021 – July 31, 2027

(b) title Renewal of CyberCorps Program at California State University San Bernardino

(c) The project recruits, prepares, supports and aids in placing cybersecurity students in positions to serve the needs of the federal government. In addition to the financial support provided through the CyberCorps for the service aspect of this program, students are immersed in professional and technical experiences to meet specific needs of both the student and the government agencies. Annual retention rate in the program was 100%. 100% of students completed internships. All who graduated received multiple job offers.

Intellectual Merit: The evaluation of the program components and its overall effectiveness contributed to the body of knowledge and best practice strategies for successful recruitment, mentorship, retention and placement of cybersecurity professionals. This program emphasized practice in the field. Under the mentorship of experienced faculty and professionals, CyberCorps students were required to work in applied activities beyond the classroom, including competitions, research and community outreach.

Broader Impact: This program provided opportunities to students from historically underrepresented groups. Students in cohorts 13 through 16 were 32% female 45% Hispanic and 19% African American. The program recruited students within CSUSB's Information Systems, Business, Public Administration, Computer Science/Engineering, and National Security Studies programs by providing a customized curricular experience to expand the pool of applicants with a diverse group of students possessing unique experiences and perspectives. By offering mentoring and support to increase the pedagogical abilities of these future professionals, and by maintaining these support mechanisms throughout their internships and in their ultimate placements, we experienced no attrition.

(d) No publications were produced under this award.

(e) N/A

(f) N/A