Cybersecurity Foundations Series: A Formative Competency- and Performance-Based Curriculum Program for Cybersecurity Education

Summary:

In compliance with the requirements of the grant solicitation, the main goal of this proposal is to produce an adaptive, performance-based, psychometrically valid, formative curriculum design that is aligned with the NSA Centers of Academic Excellence (CAE) Knowledge Units (KUs), National Cybersecurity Workforce Framework, and industry competency and capability maturity models. The proposed Core Curriculum Development Process will enable rapid deployment of adaptive curriculum that raises learner capability maturity in the foundational cybersecurity concepts, principles, and practices. The formative assessments will provide valuable pedagogical resources to cybersecurity instructors to raise learner competency levels towards mastery in each of the foundational course domains. The competency profiles produced for each learner will assist industry recruiters seeking to match talent requirements with candidate capabilities, and will facilitate articulation agreements between two-year and four-year CAE postsecondary education institutions. Finally, the adaptation of concept inventory assessment to cybersecurity education will enhance national program evaluation/accreditation and workforce planning by permitting valid aggregation and data mining of student and workforce competencies.

Background - Curriculum Standards Panel:

In 2016, the National CyberWatch Center Curriculum Standards Panel (NCC- CSP) was established. Its mission is to help identify the learning objectives, concepts, procedures, situational judgments, and intellective abilities required to develop capabilities maturity in the cybersecurity foundational principles, techniques, tactics, and protocols.

The standards produced by the NCC-CSP are the first to align instructional design, skill practice facilities, cybersecurity professional job performance standards, national workforce frameworks, and industry needs. Currently over 100 faculty, industry professionals, and government representatives have volunteered to serve on subject matter expert panels for curriculum design. Additional panel members are recruited based on their expertise and instructional experience from 228 National CyberWatch Center member organizations (128 two-year and 100 four-year) and through alliances with industry and professional associations.

Project High-Level Activities:

- Define Course Competency Domains (Topic Areas)
- Specify Assessment Rubrics for Course Competency Domains
- Specify Learning Paths and Mastery Criteria
- Develop and Assessment Plan
- Develop Instructional and Assessment Packets
- Develop Course Curriculum Map and Competency Profile
- Design Competency Profile Scorecards and Development Plans
- Implement Pilot Program to Validate Competency Profiling Designs

Curriculum Development Process:

1. Curricular design panels for learning modules are aligned with specific competencies and will be led by associate editors who have specialized expertise.
2. A panel of 20-40 subject matter experts (instructors, industry practitioners, and instructional designers) participates in identifying, defining, and reaching a consensus about important competencies.
3. Competencies are clearly defined, understood, and accepted by relevant stakeholders. Competencies are defined at a sufficient level of specificity that they can be assessed.
4. Multiple learning paths and related assessments of competencies provide useful and meaningful information to guide attainment of mastery in course content prior to advancing to Pathway Series Courses, i.e., future courses which could be developed to provide pathways to multiple careers aligned with the National Cybersecurity Workforce Framework Specialty Areas.
5. The assessment team considers precision, reliability, validity, credibility, and cost requirements in making decisions about the use of commercially developed assessments and/or panel-developed assessments.
6. The panel of experienced faculty and practitioners participate in the development of instructional designs and related assessment items (as required). A network of assessment items (prerequisites, compound items, peer and child-of relationships) will measure specific competencies forming the overall mastery learning objectives for the course.
7. The course instructional and assessment design is aligned with the developing National CyberWatch Center Core Curriculum Standards Curriculum Map. The curriculum map provides institutional guidance for course, certificate, degree, and career development pathways associated with the National Cybersecurity Workforce Framework Specialty Areas
8. Assessment items are directly mapped to learning goals in competency profile scorecards that will support individual or personalized development plans (IDP/PDP) for each learner.
9. A pilot implementation of the course enables critical decisions about strategies to improve student learning and program effectiveness. Aggregation of pilot competency profiles demonstrates a more rigorous and performance-based institutional program evaluation and accreditation process that includes formative guidance to policy makers.
10. The pilot implementation results are disseminated through public review and comment workshops to ensure all relevant stakeholders fully understand the findings.
11. The pilot implementation results are used to experiment with new ways to document students' mastery of competencies that supplement the traditional transcript.

Single Course Prototype Project Outcomes:

1. Demonstrate the rapid development and renewal of instructional materials that closely aligns with the National Institute of Standards and Technology’s National Cybersecurity Workforce Framework (NCWF) by implementing effective practices in crowdsourced,

competency-based instructional design, supporting scaling of the full program across both Foundations and Pathway Course designs.

2. Demonstrate the feasibility and agile development benefits of inductive, psychometric classification methods for identifying common misunderstandings and misconceptions of concepts, procedures, conditions, or situations, which must be remedied for accumulation of cybersecurity expertise to occur. These competency-based assessment models will apply Diagnostic Classification Modeling to produce detailed competency profiles and personalized (differentiated) learning paths for each learner as a complement to current grade-based or portfolio-based assessments.
3. Demonstrate the platform independence of the differentiated instruction modules through use in both hosted and locally established infrastructure learning environments.
4. Demonstrate the feasibility of raising the cybersecurity capability maturity levels of learners, both traditional and non-traditional, through the application of formative, mastery-based learning techniques.

Project Outcomes and Deliverables:

Outcome: Crowdsourced Instructional Designs Aligned with NCWF
Deliverables: Library of conceptual, procedural, conditional and situational instructional modules covering all NCWF Competency Areas that were designated by the National CyberWatch Center CSP as applicable for the course (draft syllabi available upon request).

Outcome: Inductive Concept Inventory Development
Deliverables: A minimum of three concept inventory assessment items will be identified for each instructional module discussed above. These will be validated and improved throughout the prototype development period.

Outcome: Platform Independence
Deliverables: The demonstration of this platform independence will be evidenced by three use-case implementations of the Fundamentals of Information Security course:
1) selective module use as a supplement to existing course syllabi using textbook or other traditional instructional techniques; 2) implementation in a standard off-the-shelf LMS which offers differentiated or mastery learning paths; and 3) implementation in a hosted environment which provides integrated, adaptive learning.

Outcome: Increasing Capability Maturity
Deliverables: Each participant in the pilot will receive a personalized competency profile showing their capability maturity within the NCWF model. This data will be aggregated to support workforce planning. Finally, a pre-post analysis will permit evaluation of maturity level increase.