I. Evaluation Plan

The evaluation team consists of an external evaluator, cyber security/cyber forensics faculty, and industry leaders who are nationally and internationally recognized in the field of cyber security. ACE will use the Evaluation Resource Center ATE Survey 2011 (Western Michigan University, 2011) as a source of information for identifying program characteristics, activities, and program impact. The external evaluation of ACE is intended to satisfy National Science Foundation requirements that all funded partnership projects conduct a thorough assessment of their activities. Project evaluation will be both formative and summative, and will play an important role in project implementation, identifying progress and next steps, and assessing whether measurable project outcomes have been achieved. The strength of the project's evaluation will come from its systematic approach: continuous data collection, interpretation, and adjustment, consistent with well-established quality principles (Westat, 2002).

The external evaluation will be led and managed by Blake Urbach-Buholz of Preferred Program Evaluations. Mrs. Urbach-Buholz has a background in educational evaluation and social science research, and has been instrumental in the development of this evaluation plan. The proposed evaluation design is based on the Standards for Program Evaluation developed and approved by the Joint Committee on Standards for Educational Evaluation to ensure that it is both thorough and comprehensive. The external evaluator will work closely with the project coordinator to review the performance assessment progress, relevant data, achievement of outcomes and deliverables to remain proactive in addressing challenges to implementation.

In addition to describing the structure and performance of the project and differences between the original intent for implementation and actual activities conducted, the formative evaluation will make recommendations intended to strengthen and coordinate project activities, design, and process. Evaluation reports will be generated semi-annually, in addition to any ad-hoc reporting that may be required. The project team has committed to reviewing the formative evaluation reports and developing an action plan to address specific recommendations under the leadership of the industry leaders.

Sample Formative Evaluation Questions	
Curriculum:	Did the project team develop a comprehensive, research-based curriculum that has been reviewed, revised, and retested?
Participants:	Were the appropriate faculty members recruited for participation? What is the demographic make-up of the student participants? Are the industry partners representative of the workforce in the region?
Process:	Did the project team follow the management plan? Did the project team implement the project as described in the work plan? What unforeseen challenges impeded adequate progress?
Correction:	What adjustments were necessary for the project's success? What corrective actions should be implemented or were implemented to meet goals, objectives, and outcomes?

In the final year of the grant, a comprehensive summative evaluation report will review programmatic activities and design, highlight the project's successes and challenges, establish the impacts on stakeholders, and guide decisions about future activities with regard to sustainability and replication. The summative evaluation will also describe the organic nature of the collaboration, uncover the project's collateral impacts on the field of cyber forensics education, and measure changes in organizational capacity across partner institutions.

Although the evaluation methods and goals are straightforward, particular emphasis will be placed on variances in performance among sites. The external evaluator will work closely with the project team to develop the tools to evaluate all objectives thoroughly. When feasible, tools will be modeled after program metrics designed by the Evaluation Resource Center ATE Survey 2011 (Western Michigan University, 2011), an NSF funded program.

The evaluation is intended to help the project better serve its constituents and the broader cyber forensics education community by documenting accomplishments and disseminating critical project-specific findings. To adequately assess the project, a holistic evaluation plan using both qualitative and quantitative measures has been developed. Data collection methods will include project records and meeting notes; stakeholder interviews; focus groups; institutional records of student performance; website analytics, and surveys of participating faculty, students, and industry partners. Coupling these methods with direct observation will provide the evaluator with a framework to understand the context within which the project operates.

Qualitative Data Sources:

1. Stakeholder interviews will be conducted semi-annually with a cross-section of the project team, participating faculty, industry partners, and other key players deemed relevant to successful project administration. This task will focus on the quality and delivery of trainings and materials, and provide an in-depth examination of the project implementation and management processes.

2. Focus groups will be facilitated annually with student participants enrolled in one or more of the core curriculum classes. Student input on the benefits, challenges, and implications of the project will provide a candid, nuanced assessment largely unobtainable through traditional surveying methods.

Participant Surveys:

1. An annual faculty survey will provide a means for tracking changes in knowledge, attitude and behavior related to participation in the online professional development activities of ACE. Survey responses will yield valuable feedback for improving the content and relevancy of materials, the method(s) of engagement, and practical classroom application.

2. A student survey will be used to solicit candid feedback from students who have completed at least one core curriculum class. Participants will be asked to describe their personal experience with the project and offer suggestions to increase student interest in and aptitude for learning the material.

3. Six to twelve months post-graduation and/or program completion, former student participants will be encouraged to share their educational or employment status via an electronic survey. This data will be used to track how many participants remain engaged in the field of cyber security or cyber forensics in various capacities.

4. An annual survey for industry leaders affiliated with the project will be designed to gauge their experience with the project, impressions of flagship activities, and suggestions for enhancing the project's ability to produce graduates who can succeed in the field.

Project and Institutional Records:

Institutions will collaborate with their respective Offices of Institutional Research to provide required data for cross-site evaluation. In partnership with the project team, the evaluator will ensure that data collection is maintained at rigorous standards. This will be accomplished, in part, by designing a user-friendly template that defines the types of data to be collected at the institutional-level and the methods for doing so to ensure uniformity across all partnering institutions. Student performance measures related to course enrollment, grades, and completion will be gathered annually by each participating institution.

PROJECT OBJECTIVES AND OUTCOMES MATRIX

Objective	Process Measure(s)	Outcome Measure(s)	Data Source(s)
1.1 Develop a rigorous curriculum that will foster an environment of learning and success in the field of cyber forensics	Implementation of a model curriculum that addresses current educational gaps within the regional context and aligns with DoD's CDFAE and NIST NICE initiatives Production and dissemination of a coherent sequence of **50** educational videos	**10** institutions will have adopted the curriculum in whole or part by project completion Faculty at each consortium institution will develop quality instructional materials tailored to their pedagogical needs	•Task completion •Project records •Website analytics
2.1 Consortium institutions will develop articulation agreements with four-year institutions	Best practices related to the design and execution of articulation agreements will be shared with consortium members	**20** new articulation agreements will be in place by project completion	•Project records •Meeting minutes
3.1 Provide ongoing professional development for faculty aimed at improving instructional practices and learning outcomes	An annual workshop will be held with faculty from consortium institutions **80%** of consortium institutions will have one or more faculty members in attendance at the annual workshop **13** faculty from consortium institutions will complete the training series in full	**80%** of faculty will report an increase in content knowledge related to cyber forensics education **4** faculty will report serving in a train-the-trainer capacity at their institution **5** principal instructors will have or receive industry credentials within 18 months of joining the consortium	•Project records •Faculty survey •Stakeholder interviews •Website analytics
4.1 Involve industry and community to grow a sustainable infrastructure that supports regional economic growth in the field of cyber forensics	**8** industry leaders will be recruited for participation in the project **25%** of industry leaders will be in attendance at the annual workshop	**80%** of industry partners will report that the project is graduating students with enhanced competencies who are prepared to enter the workforce	•Project records •Industry leader survey
5.1 Attract and advance a diverse group of students who can meet the challenges of an emerging and changing IT workforce landscape	**200** students will be recruited for participation in the project **18%** of students will self-identify as a population traditionally under-represented in STEM fields	**70%** of students will complete their core curriculum class(es) satisfactorily with a final grade of "C" or better **5%** of students will report pursuing advanced education in the field of cyber security/cyber forensics **60%** of students will seek employment in the field of cyber security/cyber forensics	•Institutional records •Student survey •Post-graduation survey •Focus groups

Objective	Process Measure(s)	Outcome Measure(s)	Data Source(s)
6.1 Evaluate the project to determine the usefulness and viability of ACE, and disseminate project findings accordingly	Formative and summative evaluation activities will be ongoing Findings and recommendations will be disseminated among consortium members	Findings and recommendations will be presented at regional or national conferences of cyber forensics practitioners Project team will submit a draft article for publication in a scholarly journal	•Evaluation reports and presentations •Publications
7.1 Establish the Cyber Warrior Program as an academic program or official school club designed to foster an environment of learning and success in the field of cybersecurity	Identification of K-12 schools prepared to implement the Cyber Warrior Program and form school-based student clubs Delivery of the rigorous curriculum to K-12 student participants of the Cyber Warrior Program	At least **5** K-12 schools will fully adopt the Cyber Warrior Program as an academic program or official school club by the conclusion of the performance period At least **50** student participants will actively take part in the curriculum or club during the performance period **70%** of student participants will increase their knowledge of cybersecurity as evidenced by their scores on a pre/post test **80%** of student participants will report that their interest in engineering, graphic arts, or technology careers has increased as a result of their participation in the program/club	•Project records •Pre/post content knowledge assessment tool •Participant satisfaction survey