A modular approach to teaching critical infrastructure protection concepts to engineering, technology and computing students

Sumita Mishra, Trudy Howles, Rajendra K. Raj,
Carol J. Romanowski, Jennifer Schneider
Rochester Institute of Technology
Rochester, New York, USA
[sumita.mishra, tmhnbs cjrcms, rkrics, jlwcem]@rit.edu

Alicia McNett
Pennsylvania College of Technology, PA, USA
amcnett@pct.edu
Daryl J. Dates
Corning Community College, Corning, NY, USA
dates@corning-cc.edu

***Abstract*—The United States Department of Homeland Security has identified 16 critical infrastructure sectors that employ computing, technology and engineering students. However, most undergraduate curricula in these disciplines do not incorporate the fundamentals of critical infrastructure protection (CIP) into their curricula in a meaningful way. This paper describes the design, development, and usage of a modular curricular framework for integrating CIP into undergraduate programs via self-contained interdisciplinary course modules; a course module is a distinct curricular unit such as a lab or teaching component for use by an instructor in existing courses without requiring any course or program modifications. The framework is designed for use in multiple disciplines, and the modules are designed for presentation at different levels of the undergraduate experience, with subsequent modules built on those presented earlier. In addition, the paper discusses assessment results obtained from the validation of the framework and modules over the past three years that covered 345 students at the community college and university levels.**

Keywords— critical infrastructure protection; course modules; interdisciplinary education; curricular assessment.

I. INTRODUCTION

Protecting the critical infrastructure during natural and man-made disasters has become a priority in most if not all countries in the world. Critical infrastructure refers to systems and assets so vital to any country that their incapacity or destruction would result in a debilitating impact on security, the economy, national public health or safety [1].

In the US, the Department of Homeland Security currently identifies 16 critical infrastructure sectors that include functions such as transportation, energy, healthcare, food and agriculture, water, financial services, emergency management, and defense, critical manufacturing and commercial facilities. Cyber resources, including the Internet, support many of these sectors; for example, the electric grid, fuel delivery systems, and water purification and delivery plants depend heavily on cyber systems. The flexibility and advantages of cyber resources are generally recognized, but they come with the constant threat of interruption, theft, manipulation, and/or destruction. Many engineering, technology and computing graduates work in such critical sectors. A compelling case can be made that these students need to learn about critical infrastructure protection (CIP) as part of their preparation. While some instructional units are available for graduate students [2], undergraduate curricula does not address CIP in any meaningful way. This paper describes a collaborative project that aims to address this shortcoming in a flexible manner.

Central to this effort is a modular curricular framework for teaching different aspects of critical infrastructure, which is then used to teach diverse engineering, technology and computing majors [3]. To support implementation in a wide variety of majors without creating new courses, the framework relies on the concept of an interdisciplinary course module as a distinct self-contained unit of curriculum; for example, a lab or teaching component. An instructor can easily insert such a course module in existing courses, without requiring any substantial course or program modifications. The framework supports use in multiple disciplines, and the modules are designed for presentation at different levels of the undergraduate experience, with subsequent modules building on those presented earlier.

This paper describes the design, development, usage and results of this modular curricular framework, along with an overview of several course modules that have been developed and delivered to students at participating institutions. The introductory CIP module has been used in various computing courses such as introductory computing and database management, as well as in non-computing courses including risk analysis, sociology, and a history of siege weapons class. Other advanced, topic-specific modules

have been developed for networking, sensor security, defensive programming and cryptography. These modules cover physical, human, and cyber aspects of CIP in appropriate detail, from introductory material to deeper, more technical concepts. In addition, the paper discusses assessment results obtained from the validation of the framework and modules over the past three years. These modules were taught at RIT and Corning Community College; this collaboration also included area high school teachers, and the introductory modules were taught at several high/middle schools, but the high school component is not a focus of this paper.

The remainder of this paper is organized as follows. In section II, the motivation for a modular framework for CIP education is described. The structure of our course modules is described in section III, and the introductory and advanced course modules developed at the authors' institutions are presented in section IV. The assessment framework and results are summarized in sections V followed by the conclusion in section VI.

II. Motivation For Using Course Modules For CIP Education

The idea of developing course modules for instruction is not unique. Modules have been used for traditional in-class instruction, continuing education and employee training. The SWEET project at Pace University aims to develop and use course modules for teaching web application security [4]. Curricular material, including labs in virtual environments, has been developed for integration in undergraduate and graduate courses. The Security Injections project at Towson University focuses on increasing student awareness and ability to apply secure coding principles through security modules that can be embedded in introductory programming and other courses [5]. The modules were designed to reflect different learning levels using varied teaching strategies as modeled by Bloom's Taxonomy [6].

Another interesting application of course modules was from Embry-Riddle, developed under an NSF grant [7]. They successfully used modules as a focused section of a course. This project showed success at using modules for a diverse audience: they used instructional materials for continuing education support for professionals, and also as introductory material for those new to the concepts. Their module packet included presentation slides, tools and quizzes.

Several instances of modular approaches to cybersecurity training exist in the literature. The National Information Assurance Training and Education Center, associated with Idaho State University, focuses on the development of training standards based on National Institute of Standards Publication 800-16 and the National Security Telecommunications and Information Systems Security Committee (NSTISSC) [8]. Eight modules dealing with Information Security are designed for integration with existing courses in a business, liberal arts or information systems curriculum.

The modular frameworks described above primarily focus on increasing cybersecurity awareness. None of them are geared towards a holistic approach covering the cyber, physical and human aspects of critical infrastructure protection. As noted by Hart and Ramsay [9], most college-level faculty acquire expertise through a combination of formal education and professional experiences. In the CIP, this approach is not currently viable because of a lack of instructors with CIP knowledge. To the best of our knowledge, our collaborative effort is the first attempt at targeting CIP instruction at the introductory formative stages of technological education, especially at the high school and undergraduate levels.

III. The CIP Course Module Framework

A course module needs to be fully self-contained so there is low effort entailed for an instructor to incorporate it into an appropriate course. Both prerequisite knowledge (input) and learning outcomes (output) need to be clearly defined. Table 1 presents the main components of a typical course module. These modules cover physical, human, and cyber aspects of CIP in appropriate detail, from introductory material to deeper, more technical concepts. Our approach builds on the work by Liu et al. [10].

Table 1: Components of a Course Module

Component	Brief Description
Overview	Description of module and prerequisite knowledge required
Learning Outcomes	Expected learning outcomes for the module
Teaching Material	Module content for instructional material or independent learning activities
Sample questions	For use in low-stake quizzes and assessment
Assignments	For hands-on experiences in solution design, implementation, and verification

The modular approach to curriculum development has several benefits, such as:

- The ability to integrate with existing lessons and reinforce current learning goals.
- The ability for instructors to use the modules to broaden the knowledge base of the students, particularly at the operational, systems and evaluation levels of understanding.
- The ability for instructors to add new modules based on learning goals and available infrastructure.
- The ability for instructors to easily modify modules to meet curricular needs.
- The ability for instructors to remove modules if resources do not exist or current student knowledge is not sufficient for a particular activity.

Although 16 distinct CIP sectors are defined by DHS, there are certain pervasive themes that can be identified across all sectors. Besides the cyber, physical and human themes that exist across these sectors, a framework based on the key elements of software, hardware, communication, and risk analysis can be developed, as shown in Fig. 1. Selected course modules are described in detail in the next section.

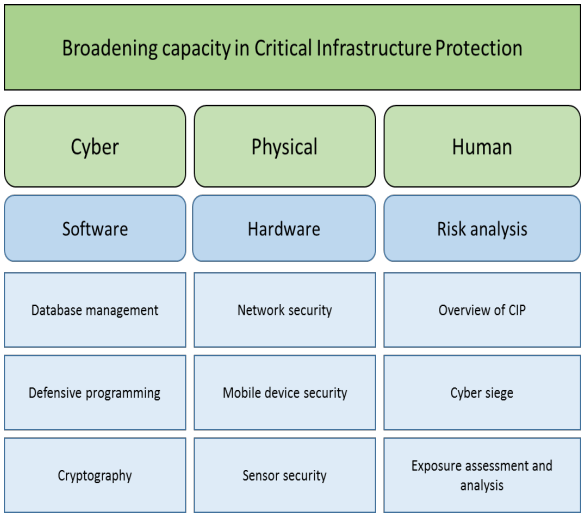

Fig. 1. Alignment of developed course modules with CIP themes

The learning outcomes of these course modules have been adapted from prior work [3, 9], and are shown below.

- **Learning Outcome 1.** Understand national strategies and policies on CIP and Key Resources – CI/KR
- **Learning Outcome 2.** Identify key components of a complex system
- **Learning Outcome 3.** Describe the hazards present in the critical components of a complex system
- **Learning Outcome 4.** Assess the level of protection and resiliency for the components of a complex system
- **Learning Outcome 5.** Learn system design concepts to achieve the desired protection and resiliency.

IV. Course Modules

Over the course of this project, we developed a wide variety of course modules across all our institutions. For illustration, this section describes two of the developed and deployed course modules to provide an understanding of the nature of these curricular units, thus paving the way to a discussion of their usage and assessment.

Additional course modules are described in the Appendix to show the breadth of our approach to course modules and their use in curricular reach across multiple undergraduate computing, engineering and technology programs.

A. Introductory Module in CIP

Overview: The physical entities and processes that make our communities function effectively are termed as critical infrastructure/key resources. Computing is a key entity that also affects several other entities. The critical resources of energy supply, water/wastewater, transportation, telecom, emergency services/medical, facilities and finance depend upon computing, and our national icons are protected by securing these networks. Simply, computing supports the delivery of these products or processes to the public or provides the tools of protection for our communities. Students will learn about critical infrastructure; its relationship to emergency management and planning; and why protecting the infrastructure is important for personal, community and national security. This module would be appropriate for any course at the high school or undergraduate levels.

Prerequisite Knowledge: None

Learning Outcomes: 1, 2

Description of curricular material: The material highlights the definition of critical infrastructure and its importance in all aspects of our daily lives. Examples include clean water supply, reliance on utilities such as power, phone and Internet, safe and reliable food supply, transportation systems, medical and health facilities, and financial services. Most people use these services every day and sometimes take for granted that they will always be available. Some situations when this might not be true include natural disasters and manmade disasters. The material also highlights the 16 CIP sectors defined by DHS and emphasizes the wide range of services and assets covered by them. The role of the individual in CIP is discussed, such as the use of strong passwords and keeping software and hardware updated. The module also discusses the three broad themes of CIP – physical, human and cyber. Examples are provided in each area.

B. Advanced Module in Network Security

Overview: The National Infrastructure Protection Plan (NIPP) and the Department of Homeland Security (DHS) outline several areas of protection for federal networks and critical cyber-infrastructure [11]. Switches and routers are critical components of the infrastructure. Students learn the strategies and requirements for basic security of layer 2 and layer 3 devices and understanding lower-level cyber-attacks. Topics covered include plain text passwords, user-level security, port security, access-list protection, and layer 2 and layer 3 specific attacks on switches and routers, and how they have an impact on the overall protection of the critical infrastructure. This module would be appropriate for a second year course in computer networking.

Prerequisite Knowledge: Introductory Module in CIP

Learning Outcomes: 3, 4, 5

Description of curricular material: The material integrates the awareness of CIP in the networking course material. Any piece of networked infrastructure can become critical based on its geographic location and end-user functionality. It is very difficult to model real-world scenarios of CIP without dedicating considerable amount of time to planning, building, and analyzing the infrastructure. The proposed modular approach helps to alleviate some of these problems. This approach works on the principle that each student (or student group) is able to manage his or her own "module" of a larger topology. The modular topologies are fairly simple and related to the concepts that are taught in regular networking courses, but they are able to simulate the situations that these students may face in a real-world environment. Each topology is then evaluated based on the NIPP Framework [11], the NIST framework [12] and the Communications Sector Specific Plan [13], with thought-provoking questions provided to guide them toward thinking about CIP. Additionally, the modules can be interconnected to simulate the dependencies and challenges that surrounded disparately owned elements of critical infrastructure.

V. Assessment Framework and Results

Project assessment covered the module content, the instructional effectiveness of each module, and faculty development and growth in CIP-related areas. Table 2 lists our evaluation plan used to determine the effectiveness of the modular content and instructional effectiveness. The modules were deployed and evaluated over a three-year period.

For the first year project review, instructors gathered data from post-delivery discussions, or one-on-one conversations with students. This data revealed some common questions and comments:

- I know this is important, but how does this relate to me?
- What is ***my*** role in protecting the infrastructure? Give me examples.
- For computing students: I need to understand more about how computers tie into CIP.

Several modules were adjusted, especially the introductory module, which provided an overview of the infrastructure, personal behaviors, and basic cyber threats. The introductory module was used as a prerequisite for advanced modules to ensure that all students were introduced to the basics. Students were asked to take a pre- and post-delivery survey; the survey was used to measure students' initial understanding, and the impact of the introductory material. The pre and post tests were delivered several days apart to help determine retention of the material.

For the introductory module, students were administered pre- and post-tests, with two common questions on both tests:

- **Question 1**: List one personal "bad behavior" that may compromise the critical infrastructure.
- **Question 2**: List one reason why there is great concern for protecting the critical infrastructure.

Table 2: Evaluation Plan for Curricular Goal

Evaluation Questions	Data Source	Data Collection	Analysis
1. How easily and effectively are modules integrated into existing curricula?	Design teams and adopting instructors at year level and discipline	Lesson plans and curricular material. Instructors' feedback rating useful component modules, ease of use, time to introduce the topic, and appropriateness of indicated module prerequisites	Expert review from instructional designers and instructor feedback to provide critique and suggestions
2. Are modules effective for students at each year level?	Students aggregated by year level	Aggregated learning gains at each level	Determine differential effectiveness by audience level
3. How effectively are students in different disciplines learning the intended outcomes of each module?	Students who participate in the initial modules	Direct assessment of knowledge and skills with post-tests for each module	Between-group comparison of average achievement between different discipline groups (computing, technology, engineering majors)
4. Are the modules designed and delivered appropriately for each educational level?	Sample from each level	Individual interviews regarding student perceptions of module delivery, value, and content	Interview summaries and content analysis by evaluator
5. To what extent is each of the five CIP learning outcomes attained?	Achievement data from each module that contributes to each CIP learning outcome	Direct assessment of knowledge and skills with post-tests for each module	Aggregate success by CIP outcome

These common questions were used to gauge student understanding and appreciation of the material across all courses. Additional questions on the tests were specific to the course in which the module was taught.

As part of the assessment, we analyzed feedback from 206 community college and university students taking the introductory module. Table 3 shows student demographics.

TABLE 3: STUDENTS DEMOGRAPHICS FOR THE INTRODUCTORY MODULE

Course Type	**Number of Students**
Computing Courses	133
Non-Computing Courses	73
Total	206
Student Type	**Number of Students**
Community College	50
University	156
Total	206

As was expected on the pre-test, most students were vaguely familiar with CIP-related issues, with most familiarity based on news reports of current threats and incidents. Students had a somewhat superficial understanding of the breadth of the issues and target areas, and the potential ripple effect when even one critical system is compromised. The initial results of the pre-test showed that students were minimally aware of the concerns for protection of the infrastructure with only 34% able to correctly identify why there is concern for protecting the infrastructure. Also on the pre-test, students were asked about personal behaviors and the infrastructure. This issue was even less understood with only 20% able to initially cite a "personal bad behavior" that could contribute to compromising the critical infrastructure.

A separate analysis examined pre and post-test results for computing and non-computing classes to determine if a previous computing background impacted students' perceptions of CIP. The data analysis showed no statistically significant difference between the pre-test scores of computing classes compared to non-computing classes ($t=0.0$). There was, however, a statistically significant difference in post-test scores of the same two groups with computing students achieving higher overall results ($t=3.48$).

The Introductory Module appears to have created a basic awareness (based on the comparison of student pre and post-test scores) and discussions in the classes (Instructor Evaluations). This data suggests that students' awareness increased significantly from the pre-test to the post-test. However, many student responses were individualized, focusing on very personal issues such as password protecting a cell phone or using strong passwords. Based on this data, it is not possible to determine how many students grasped the importance of the critical infrastructure in the "big picture" look at the problem.

Advanced CIP modules were developed for use in upper-division courses. These advanced modules were taught in several upper-division computing courses including sensor networks security, data management, computer security, cryptography, networking fundamentals, systems analysis, and defensive programming. Students first learned the materials in the introductory module, and then studied the advanced module's subject-specific content. For example, in a computer security course, the instructor emphasized database security and the need to track the content and status of CIP structures so they can be protected during a crisis. The defensive programming course focused on common misconceptions and programming errors; assignments challenged students to uncover vulnerabilities in existing code.

The advanced modules were taught to a total of 139 students. Since the content varied based on the course, most instructors evaluated the module content based on unit or final exam questions, and others assigned projects, papers, or posters. In other words, it was not possible to conduct a common assessment across all of these advanced modules.

One trend that did seem to emerge was that student maturity and experience impacted appreciation of the material. As shown with the introductory modules, students' perceptions were very personal–protecting my cell phone or my email account. Instructors teaching the advanced CIP modules indicated that students with more experience such as previous course work or cooperative work experiences had a much stronger appreciation of the issues and potential consequences.

An instructor teaching the Computer Security module noted that many students had recently completed a course on basic data management. The instructor commented that students with the previous database background seemed to better understand the issues and dangers involved. Would the advanced modules be best suited for specific courses where students have already learned associated trends and technologies? These results are purely suggestive, and need to be further explored to better understand the role of modules in curricular development.

Another important component of this effort was outreach to instructors through a one-day seminar. Attendees spent the morning in sessions learning the introductory and mobile device security modules. The afternoon sessions were more technically advanced, with a focus on securing the cyber infrastructure (login, networks and resiliency), and defensive programming. The day's sessions concluded with an open discussion, and attendees were asked to complete a workshop survey.

Clearly, the hands on focus of the workshop demonstrated the serious nature of the subject, but some attendees admitted they were most comfortable with the introductory materials and felt unprepared for participation in higher level technology tasks. In general, the attendees provided very positive comments on the workshop, and a request was made for a multiple day "boot camp." All attendees were provided with a full packet of information including reference slides for each session and materials for delivering the modules.

All educational materials are available at the project's website at http://nsf_cip.csec.rit.edu/. Posted at this site are the slides and instructor handbooks for the introductory and advanced modules, survey instruments, and details of the instructor workshops. This site also contains links to other project details.

VI. CONCLUSION

Recognizing the need for CIP-trained professionals, a cross-disciplinary team of faculty across three institutions developed the module-based strategy for introducing CIP in the undergraduate curriculum. This effort started with course modules to introduce necessary concepts and theoretical backgrounds, and was extended to build a framework of self-contained instructional modules. Our assessment results indicate that there exists both a need and opportunity to integrate CIP across the undergraduate technological curriculum. As the use of technology becomes more ubiquitous, at ever younger ages, we must seek opportunities to imbue this awareness to all users of technology, so that their view of the role of technology and its possible impacts reflects the actual risks we face in terms of CIP.

ACKNOWLEDGMENT

This material is based upon work partly supported by the National Science Foundation under Award DUE-1303269. The authors would like to acknowledge the support of Fred Rion, Emergency Preparedness Administrator, and the Rochester (NY) Metropolitan Statistical Area's Urban Area Working Group. The authors would also like to acknowledge the ongoing support of the NYS Department of Homeland Security and Emergency Services.

APPENDIX: ADDITIONAL COURSE MODULES

As stated earlier, this appendix provides the descriptions of other course modules we have developed and deployed in our teaching. They are provided here for completeness, and show the extent of our work in supporting a diverse set of undergraduate (and high school) curricula.

A. Advanced Module in Defensive Programming

Overview: Software is a critical component of any cyber-infrastructure. Defensive programming involves safeguarding software and its corresponding data against both unintentional and intentionally produced errors. Hackers exploit vulnerabilities in order to misuse software, while others may simply interact with software in ways not intended by the programmer, producing unwanted behavior. Consequences of these interactions include stolen data, questionable data integrity, loss of privacy, poor user experience, and other costly errors. Unfortunately, all software is susceptible to these bugs and security hazards; defensive programming helps to proactively safeguard software and prevent these consequences from occurring in the first place. During this module, students develop awareness of issues surrounding software security and learn about basic defensive programming techniques. Awareness is developed by examining several real-world scenarios where vulnerabilities proved costly to an organization and their customers/users. The module explores common programming errors, followed by a discussion of programming best practices. While some of the practices presented are quite simple, others are slightly more advanced, but presented in a manner that those in an introductory programming class should be able to comprehend, making this an ideal module to integrate into introductory programming courses.

Prerequisite Knowledge: Introductory Module in CIP

Learning Outcomes: 5

Description of curricular material: The material highlights the definition of defensive programming and its importance in a variety of systems. Examples include financial, commercial, healthcare, and communication systems, all types of systems critical to our infrastructure [1]. Common misconceptions surrounding defensive programming are debunked and common programming errors are explored in order to help build student awareness of these issues. This material is then followed by recommended best practices and hands-on labs that provide students with firsthand experience with the consequences of code written in a non-defensive manner. Seed questions to spur group discussions are also provided.

B. Advanced Module in Cryptography

Overview: Students unknowingly interact with cryptography and encoding mechanisms on a daily basis when searching the Internet, making a purchase online, or using their password. This module demonstrates and explains what is happening behind the scenes with non-technical hands-on activities and computer-based demonstrations. This module would be appropriate for a first or second year computer course for computer majors or non-majors.

Prerequisite Knowledge: Introductory Module in CIP

Learning Outcomes: 2, 3, 4

Description of curricular material: This module discusses the risks involved in communicating over untrusted channels using the example of ecommerce transactions over the Internet. A brief history of cryptography and a simple weak cipher is discussed, with several hands-on activities accompanied by examples of using crypto analysis and brute force to attack the cipher. Encoding, encryption, and hashing are introduced and contrasted. The primary activity demonstrates the differences between symmetric and asymmetric cryptography, and the mechanisms that are used to protect data when conveyed over untrusted networks, such as private keys and certificate authorities. Cryptography supports not only the secure authentication of users, which is an important element of Critical Infrastructure Protection, but also the security of critical communication channels. These encrypted communication channels may be used for secure commerce as well as the remote control and monitoring of industrial processes and critical infrastructure such as energy production and water distribution.

C. Advanced Module in Cyber Siege

Overview: Throughout history sieges have been a common form of warfare. The basic strategies of physical siege

warfare have not changed over the centuries, although defensive and offensive weaponry advanced considerably. In the 20th and 21st century, however, a new type of siege emerged—the cyber-siege. This module explores the history of cyber-attacks, discusses the attackers and their targets, and shows how, just as in the past, offensive tactics drive defensive advancements and vice versa.

Prerequisite Knowledge: Introductory Module in CIP

Learning Outcomes: 3, 4, 5

Description of curricular material: The module consists of explanatory material and several case studies of recent high profile cyber sieges, including the methods used by both defenders and attackers. In homework assignments, students compare and contrast physical siege strategies with those used in cyber sieges, including the influence on human behavior on both sides of the conflict.

D. Advanced Module in Database Management

Overview: Database systems have been used for the past few decades and are now an integral part of the basic infrastructure used in all 16 critical infrastructure sectors. In addition, database systems play a vital part in helping to protect critical infrastructure by identify different aspects of each infrastructure system, for example, identifying storage locations and types of chemicals in a neighborhood so that emergency management personnel are aware of them when deploying fire trucks or ambulances during an emergency. This module demonstrates and explains how database systems can help to support critical infrastructure during normal operations and protect it during emergencies. This module would be appropriate for use in a second or later year computer course for computing majors.

Prerequisite Knowledge: Introductory Module in CIP

Learning Outcomes: 1, 2, 3, 4

Description of curricular material: The module consists of explanatory material about database systems, and their use in building software systems used to support critical infrastructure. It also covers the development and usage of specific databases to identify and store information about critical infrastructure that become crucial in protecting systems during emergencies. Issues relating to data security and privacy, and how they change during emergencies are also presented.

E. Advanced Module in Exposure Assessment and Analysis

Overview: This module builds upon the introductory module described earlier, and seeks to teach the connection between assessment of operational risk with the computing and system vulnerabilities inherent in the operation of critical infrastructure. Students will examine the process of risk management through the lens of infrastructure as the key systems of our community. This module is targeted at engineering and management students who have a foundation in management of risk and would be appropriate at the undergraduate levels.

Prerequisite Knowledge: Understanding of risk management

Learning Outcomes: 1, 2, 3

Description of curricular material: This course examines risk exposure and vulnerabilities in all genres, including hazardous products and materials, process risk, and operational risk. It requires students to assess potential vulnerabilities and unknowns and formulate plans for ongoing corporate risk management. In this sense, it has a unique view of CIP, and particularly speaks to those who will be the future managers of operational systems and business continuity.

REFERENCES

[1] U.S. Department of Homeland Security, "What Is Critical Infrastructure?" Accessed: 10 April, 2016. http://www.dhs.gov/what-critical-infrastructure.

[2] George Mason University Center for Infrastructure Protection and Homeland Security. Accessed: 10 April 2016. http://cip.gmu.edu/education-programs/critical-infrastructure-higher-education-initiative/.

[3] S. Mishra, C. J. Romanowski, R. K. Raj, T. Howles, and J. Schneider, "A curricular framework for critical infrastructure protection education for engineering, technology and computing majors *IEEE* Frontiers in Education Conference *(FIE)*, Oklahoma City, OK, 2013, pp. 1779-1781, 2013 pp., Oct. 2013.

[4] L. Tao, L. Chen and C. Lin, "Improving Web Security Education with Virtual Labs and Shared Course Modules," *IEEE Frontiers in Education Conference (FIE),* pp. F2F1-F2F3, Oct. 2010.

[5] B. Taylor and S. Kaza, "Security injections: modules to help students remember, understand, and apply secure coding techniques," *16th annual joint conference on Innovation and technology in computer science education*, pp. 3-7, 2011.

[6] D. R. Krathwohl, "A Revision of Bloom's Taxonomy: An Overview" Theory Into Practice, Volume 41, Number 4, 2002.

[7] S. Gerhart, M. Jaffe, P. Hriljac, R. Sobotta, J. Hogle and R. Bloom, "Increasing Security Expertise in Aviation-Oriented Computing Education: A Modular Approach," NSF Award DUE-0113627, 2001.

[8] National Information Assurance Training and Education Center. Accessed: 11 April 2016. http://niatec.info/ViewPage.aspx?id=0.

[9] S. Hart and J. Ramsay, "A Guide for Homeland Security Instructors Preparing Physical Critical Infrastructure Protection Courses," Homeland Security Affairs 7, Article 11 (April 2011). Accessed:11 April 2016. https://www.hsaj.org/articles/59.

[10] X. Liu, R. K. Raj, T.J. Reichlmayr, C. Liu, and A. Pantaleev, "Teaching Service-Oriented Programming to CS and SE undergraduate students," *IEEE Frontiers in Education Conference (FIE)*, Oklahoma City, OK, 2013, pp. 15-16, 2013.

[11] US Department of Homeland Security, National Infrastructure Protection Plan (NIPP). Accessed April 11 2016. http://www.dhs.gov/national-infrastructure-protection-plan/.

[12] NIST Framework for Improving Critical Infrastructure Cybersecurity. Accessed April 11 2016. http://www.nist.gov/cyberframework/.

[13] NIPP Communication Sector Specific Plan (SSP). Accessed April 11, 2016. http://www.dhs.gov/communications-sector/.