Curriculum Development for Teaching Critical Infrastructure Protection

David Oliver
University of Idaho

Michael Haney
Assistant Professor, CS Department
University of Idaho

Abstract - The critical infrastructure of the United States, from the electric grid to transportation, agriculture, and financial and government sector systems, has simultaneously grown more vast and more complex. So too has the challenge of protecting the infrastructure as an intertwined and interdependent system of systems. Recent years have seen a shift in perception and a growth of importance in critical infrastructure protection (CIP). The nature of the complexity of these systems and interdependency of sectors necessitates a multidisciplinary approach to educating the workforce needed to protect them. This paper outlines the objectives and efforts at one university to build a graduate-level curriculum that seeks to bridge the knowledge and communications gap between once stove piped educational disciplines: 1) information assurance and cybersecurity from the Department of Computer Science, 2) sector-specific engineering from the Departments of Electrical Engineering, Mechanical Engineering, Civil Engineering, and Environmental Science, and 3) infrastructure protection and homeland security from the Departments of Industrial Technology and Engineering Management. The efforts to date include the creation of a new cross-discipline course covering the fundamentals of critical infrastructure protection and the creation of a new graduate certificate. The certificate has been formed by requiring the new fundamentals course as well as a series of elective courses from various disciplines chosen for meeting several distinct and specific learning objectives. The certificate program further serves as a roadmap of elective courses to be used by students pursuing a Master's degree in various engineering disciplines. The specifics of these requirements as well as our motivations for choosing them are described in this paper.

1 INTRODUCTION

The concept of critical infrastructure originated in a form much different from how it is perceived today. Critical infrastructure began offensively, as a military designation of a high-value civilian bombing target during World War II [1]. Planners would rank targets and plan missions based on the debilitating effects the loss of those targets would cause. Since that time, and in the absence of a 'Total War' effort, critical infrastructure has morphed into a defensive strategy to protect and perpetuate the way of life for a nation's citizenry.

The visibility and importance of Critical Infrastructure Protection (CIP) has increased dramatically over the last 2 decades. In 1996, President Clinton ordered that a commission be assembled to investigate and analyze the current state of critical infrastructure nationwide and propose a path forward to protect it [2]. The report delivered by that commission concluded succinctly that "Waiting for disaster is a dangerous strategy. Now is the time to act to protect our future [3]." The commission's warning has grown sharper in hindsight after disasters such as the terrorist attack on September 11, 2001, Hurricanes Katrina and Sandy in 2005 and 2012, respectively. These events have offered significant opportunities for us to learn and improve our protection of critical infrastructure through preparation for inevitable future manmade and natural disasters.

One of the primary roles of Academia in support of critical infrastructure protection is educating the future workforce. As educators, our goals include developing and maintaining the best possible curriculum for the widest audience to impart the knowledge and skills necessary to defend our nation's critical infrastructure. However, just as the infrastructure is highly complex, so too is the nature of a curriculum designed to cover all the nuance of its protection. Many different roles must be filled, and the material necessary to prepare students for these roles comes from many different corners of the university. The challenge at hand is how to organize it and make it available to current and future students.

2 NATURE OF THE NEED FOR A MULTI-DISCIPLINED CURRICULUM

Protecting critical infrastructure is a difficult problem given the size, complexity, and interdependencies among assets, systems, and public and private organizations. While it is well known that critical infrastructure assets are interdependent, the full extent of those interdependencies has not been adequately identified. The Department of Homeland Security Office of Infrastructure Protection (IP), Infrastructure Information Collection Division (IICD) has taken a lead in identifying infrastructure interdependencies with the All Hazards Analysis (AHA) framework, but this is a relatively recent initiative and will require years to evaluate the tens of thousands of publicly and privately-owned facilities and systems that together comprise US critical infrastructure [4]. Critical infrastructure interdependencies and fault chain analysis are areas of active research.

Attempts have been made to formalize the skills required to protect critical infrastructure into a common body of knowledge (CBK) [5]. These efforts have not yet fully captured the attention of educators or been translated into widespread acceptance of critical infrastructure protection as a formal field of study. This is most likely due to the size and complexity of the problems, and that they do not clearly fall into a single college department for the purpose of awarding either a four-year undergraduate or graduate degree. Government continues to document the need to protect the systems and infrastructures that make modern life possible, and industry will need to rise to meet the challenges. Academia must play its role in research and development of curriculum necessary to support industry demand [6].

2.1 Multidisciplinary Aspect of CIP

The major challenge that infrastructure protection professionals will face is managing the size and complexity of not just a given operational asset, but the interdependencies of these assets within and across various sectors. Currently critical infrastructure in the US is divided into 16 sectors, each employing engineers from various disciplines as well as cybersecurity professionals. The vulnerabilities

impacting critical infrastructure, both physical and cyber, are also varied. Some of the vulnerabilities are specific to a single sector while others cut across all sectors. A one-size-fits-all approach to teaching infrastructure security and protection would need to be overly complex or insufficient in its breadth and depth, and we feel it ultimately will not work. A broad approach to understanding the basic needs of infrastructure protection could be the focus of an introductory course, but this would leave industry the burden of providing training for the professional at appropriate levels of detail in sector-specific knowledge. As an example, our university like many others currently offers a course in Supervisory Control and Data Acquisition (SCADA) security issues, taught by faculty from the computer science department. As such, it provides a cursory overview of some hardware equipment and focuses on the strengths of both the instructor and the CS-major students. It often lacks sufficient coverage of engineering domain-specific requirements, constraints, and nuance.

2.2 Our Curriculum and Learning Objectives

The goal of our proposed curriculum improvements is to help meet the overwhelming demand for skilled workers in a broad range of engineering and security positions supporting the protection and resilience of the nation's critical infrastructure sectors. Our university's current offerings in the area of cybersecurity, information assurance, and cyber-physical systems protection is, like many schools with similarly focused programs, focused on computer science and computer security issues. However, there is a growing realization that cybersecurity education needs to be made available to a wider range of engineering and technology students, and that engineering and technology issues that are often covered in other departments and disciplines, including electrical, mechanical, and civil engineering, need to be understood by the computer science students focused on cybersecurity. Hence, a primary aim of our efforts is to cross-pollinate these populations of students.

We have identified several key learning objectives which we would like to accomplish through a combination of enhancements to existing curriculum and creation of new courses. The form of these curriculum enhancements is discussed

in a later section, but first we articulate the goals of the effort. 1) The first learning objective for students focused on critical infrastructure is to achieve a sufficient level of understanding of the core concepts of society's critical infrastructures, the systems of systems which comprise them, and the issues involved in managing these systems and their interdependencies. 2) The second objective is for students to obtain an understanding of the elements and methods of assessing and managing risk and their applications. 3) The third objective is for students to develop knowledge of key concepts of resiliency, security, and assurance, and of how to apply these concepts, tools, and techniques to people, processes, and technologies. 4) The fourth objective is for students to develop a deeper understanding of the operations of one or more critical infrastructure sector technologies (e.g., water systems, transportation systems, or energy systems, including electrical power systems, petroleum, or nuclear power). 5) The fifth objective is for students to obtain a strong skillset in one or more areas of cybersecurity (e.g., network security, systems security, incident response, forensics, or reverse engineering). 6) The final learning objective for students is to synthesize the information from these various courses through the efforts of a capstone project. Combined, we believe students with this level of exposure to both breadth and depth of information will be far better prepared to face the challenges of protecting at least one critical infrastructure sector's systems and assets.

No.	Learning Objective	Means
1.	Critical Infrastructure	Fundamentals of Critical Infrastructure (new course)
2.	Risk assessment / management	Choose one existing course (e.g. TM – Risk Management)
3.	Security, assurance, resilience	Choose one existing course (e.g. CS – Advanced Information Assurance)

No.	Learning Objective	Means
4.	Domain-specific engineering and cyber-physical systems	Choose one existing course (e.g. EE – Resilience in Power Systems)
5.	Cyber-security technical skills	Choose one existing course (e.g. CS – Forensics)
6.	Sector-specific analysis	Capstone project

Table 1. Learning Objectives for Critical Infrastructure Protection Curriculum

3 SURVEY OF CURRENT CURRICULUM OFFERINGS

For this effort, we sought a model curriculum consisting of one or many courses from which to draw inspiration, structure, and material. An examination of current course offerings, while not exhaustive, was surprising in how few centers of higher education in the United States advertise curricula in the area of infrastructure protection, security, or resilience. Many schools offer courses in security topics, most often in computer science or computer engineering disciplines and sometimes related to cyber-physical systems. But very few pull together various disciplines of engineering, coupled with policy, and take a broad view of US critical infrastructure. A brief overview of some of the university, government, and commercial courses follows. The identified courses were evaluated as a fit for a course or curriculum model to meet our stated objectives, and any deficiencies noted here relate only to those criteria.

3.1 FEMA Emergency Management Institute

The Federal Emergency Management Agency (FEMA) Emergency Management Institute (EMI) offers a selection of classroom-based and online courses from its headquarters in Emmetsburg, MD [7]. The EMI courses focus

almost exclusively on preparation for and handling of natural and manmade emergencies, consistent with their charter. The FEMA course most closely lined with our goals, entitled "Critical Infrastructure Security and Resilience: Achieving Results through Partnership and Collaboration" is a two-hour course with a focus on community relationships. It lacks the depth required for our needs.

3.2 DHS ICS-CERT

The US Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) offers eighty hours of online and in-person training from their facility co- located with Idaho National Laboratory in Idaho Falls, ID [8]. Subjects ranging from operations security (OPSEC) to tactical cybersecurity defense are covered, with the final class in the sequence culminating in a 12 hour "red-blue" adversarial exercise similar to many "capture-the-flag" events. This event consists of a "blue" team of enterprise defenders tasked with managing the ongoing operation of cyber-physical process, an internal corporate network of web servers, file and print services, directory services, and user workstations, as well as a security team with firewall and network monitoring capabilities. The "red" team is given access to an "external" network and all the tools and techniques they can muster to try and penetrate the blue team's defenses and disrupt the cyber-physical processes.

The ICS-CERT training focuses on specific types of attacker tactics and defense in an abstract 'all- sectors' network. The ICS-CERT training is available internationally for industry professionals and is in high demand. However, it is a small program with a limited reach and does not examine some of the context for how US critical infrastructure protection efforts have evolved over time. Further, the material assumes an existing knowledge of domain-specific engineering in one of the 16 critical infrastructure sectors, as it is targeted at working professionals from asset owner organizations. It provides a "crash course" approach to cyber-security concepts and tools, such as network mapping, system scanning, and using metasploit.

3.3 DePaul University

In 2013 Luallen and Labruyere [9] discussed similar goals and learning objectives, outlining their efforts and reasons to create a course in Critical Infrastructure and Control Systems. Citing the need to "empower the next generation of cybersecurity professionals, engineers and executive leadership", they focused on introducing the security of controls systems into their existing computer science curriculum. They prototyped and deployed a "Portable Living Laboratory Kit" which included networked PLCs in a configuration consistent with industry practices. Using that kit, they were able to build PLC-centric exercises intended to demonstrate attack and defense strategies students might encounter upon joining the workforce. While these skills are essential, the course as a whole seems to lack the cross-discipline breadth we are seeking in a model for teaching critical infrastructure resilience. As with many other courses of a similar nature, the material appears to take an appropriate deeper look at cyber-physical control systems security, but lacks coverage of the broad and complex nature of critical infrastructures and their interdependencies.

3.4 Naval Postgraduate School

The Naval Postgraduate School hosts a Master's program that is available at no cost to Federal, State, Local, Tribal, & Territorial (SLTT) employees [10]. Offered through the Center for Homeland Defense and Security, the NPS Homeland Security Master's degree is only available to employees of any level of government. We were unable to obtain syllabi or course materials for comparison.

3.5 University of Idaho

The University of Idaho currently offers a graduate certificate in Secure and Dependable Computing Systems (SDCS) [11], similar in scope to the current effort to increase critical infrastructure resilience. Offered through the Computer Science (CS) Department since 2001, this certificate enabled CS Master's students to understand the security issues of hardware and software in systems ranging from

standard IT products to embedded systems and microcontrollers. The exponential growth of internet-enabled industrial control systems, cyber-physical systems and the Internet of Things (IoT) has created a large demand for cybersecurity professionals that have an understanding of fault-tolerance and survivability, both topics that are part of the SDCS certificate. However, as with other offerings, this certificate requires only CS courses, along with a significant number of CS prerequisite courses, making it inaccessible to students in other engineering disciplines. In addition, students are not exposed to the larger context of the policies, risk assessment methodologies and domain-specific challenges that constitute the current state of critical infrastructure.

3.6 Mississippi State University

Mississippi State University (MSU) built a bench-scale SCADA security laboratory incorporating commercial software and hardware able to simulate a variety of real-world industrial processes [12]. More than a research laboratory, MSU proceeded to create courses using it as the main focus of the course as well as adapted existing courses to incorporate SCADA security concepts with hands-on experience. MSU has also created short courses for industry professionals needing training on specific systems or technologies such as Smart Grid. While this level of effort is beyond the budget for the work we are pursuing, it is impressive and helped us realize that a hands-on approach might be valuable within the scope of our efforts.

3.7 George Mason University

George Mason University (GMU) Center for Infrastructure Protection and Homeland Security (CIP) published a series of stand-alone courses covering a variety of topics in the critical infrastructure protection domain as part of their Higher Education Initiative. These courses have been made available for any university to incorporate into an existing program or to create a new one [13]. GMU in 2014 released a package of courses as a fifteen-credit graduate certificate. Upon reviewing the course materials we decided that the GMU Foundations of Critical Infrastructure Security and Resilience provided the broad-based exposure

to critical infrastructure resilience topics we were looking for in a model for the basis for our curriculum. However, the GMU curriculum is heavily focused on policy and administrative aspects of critical infrastructure, as its target audience appears to be working professionals that are managers or policy setters. The courseware provided lacks the depth of material that focuses on cybersecurity issues or domain-specific engineering concepts that would be required of workers tasked with securing and ensuring the resilience of cyber-physical industrial control systems.

4 PEDAGOGY

Based on the findings of this background research, and the goals for critical infrastructure education we initially outlined, this section describes our approach to tackling this pedagogical challenge. In order to meet our stated learning objectives, we have chosen to develop a new cross-disciplined multi-course graduate certificate. This certificate draws from our existing courses across the university from several departments and combines them through a selection of specific elective courses chosen to meet one of the four stated target outcomes. However, our existing university curriculum did not sufficiently cover the core fundamentals and broad view of critical infrastructure and homeland security issues. This is where we began by creating a new course which would form the foundation of the curriculum.

4.1 New Course on the Fundamentals of Critical Infrastructure Resilience

Using the GMU course offerings as an initial model, a new course titled "Fundamentals of Critical Infrastructure Resilience" (hereafter referred to as *Fundamentals*) was developed. *Fundamentals* seeks to expose students to the breadth of the current unofficial but extensive body of knowledge on critical infrastructure protection with enough depth to understand the interrelationships of the laws and regulations that undergird US policy. *Fundamentals* is comprised of twelve modules over a sixteen-week semester. The course draws its materials from a number of sources, and for the first semester we plan to use the textbook *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* by Ted Lewis and published by John Wiley & Sons [14]. The text takes an in-depth look at the history

and evolution of US critical infrastructure policy and protection as well as the current state of CIP in each sector. The breadth and depth provided by the text seems to fit our needs. We will evaluate the text at the end of the first semester to determine whether we will continue to use it.

The course will also require selected readings taken from US federal government documents, such as regulations and legislation (e.g. the National Infrastructure Protection Plan of 2013), executive orders (e.g. Presidential Decision Directive 63 of 1998), NIST standards and inter-agency reports (e.g. SP 800- 82 r2), and academic papers and opinion pieces from all levels of government, academia, and private industry [15-17].

Modules include the following topic areas:

- Defining and achieving critical infrastructure security and resilience (CISR)
- History of US critical infrastructure protection to date
- CISR in the 21st century threat environment
- CISR authorities, roles, & responsibilities (Federal, SLTT, Private Sector)
- Information sharing
- Assessing CI risk
- Enabling CISR through either a voluntary or regulatory approach
- Insider threats
- SCADA and other cyber-enabled systems vulnerabilities
- International CISR
- All-hazards approach to CISR
- Long-term & enduring risks to CI

Fundamentals is designed to be taught either once or twice per week in longer classes that support class discussions. Module lectures are delivered in one class in the week, or during half of a longer once- weekly class. Readings are assigned for

the following class. A follow-up discussion of topics and reading assignments occurs the following class period. A quiz for each module has been developed to gauge comprehension of the assigned readings (and to encourage students to complete the reading assignments prior to coming to class). Classes will also include student project presentations and reactions to the readings. This model follows the "flip the classroom" model proposed by Bergmann and Sams [18].

While this course is new, as it is taught over subsequent semesters, the lectures will be recorded and assigned to watch prior to class, so that class time can focus on group discussions and project development.

4.2 Fundamentals Course Final Project and Exercise

To reinforce the real-world applications of the course, the university has partnered with local critical infrastructure operator organizations to undertake an exercise as the capstone event of the semester. The local provider of electricity for a community of 65,000 customers has agreed to participate in the exercise at the conclusion of the next semester course. The students will design a tabletop exercise (TTX) for use by the company officials, developing a disaster scenario with input from local subject matter experts intended to exercise the company's incident response procedures. Developing the exercise will be a divided into a number of group efforts, and the class will administer the exercise for the target company personnel. The exercise is anticipated to last 4 hours. Afterwards, each student will be required to write a short (i.e. 3 to 5 pages) After-Action Report (AAR) detailing the execution of the exercise and all lessons learned. These AARs will be presented to an audience of the instructors, classmates, and officials from the utility company.

4.3 Graduate Certificate and Curriculum Roadmap

While the *Fundamentals* course provides a broad spectrum of information for learners and identifies the means by which additional information can be obtained, our goals include taking a deeper dive into the technical aspects of protecting critical infrastructure cyber-physical systems. The purpose of the required *Fundamentals*

course is to expose the learner to various aspects of infrastructure protection, many of which are lacking in other curricula we examined. We recognize that the depth and breadth of the information available exceeds the scope of a single course, and the complexity defies being housed in a single department or degree program which forces students into a particular specialization. We are proposing a new multi-disciplined graduate certificate in Critical Infrastructure Resilience to address this need. Our approach is to draw from existing available courses and group them in such a way that students meet our targeted learning objectives.

The new Critical Infrastructure Resilience graduate certificate is attainable by a large audience of students and working professionals. It dovetails with three Master's degree programs offered at the university. The certificate provides the elective coursework for Master's degrees in Technology Management (TM), Computer Science (CS) or Electrical and Computing Engineering (ECE) currently available. That is, students can choose the majority of electives from their current disciplines, adding a cybersecurity course from the CS department and the *Fundamentals* course as electives in their study plan. As a graduate certificate, it is also attainable without pursuing a full Master's degree. The diversity of disciplines within the cross section of students will foster dialog and comparison of methods of infrastructure protection across critical infrastructure sectors. We feel this approach will provide both depth and breadth to students over a five-course curriculum that bridges gaps between computer science professionals, field operators, technicians, engineers, and managers.

4.4 Required and Elective Course Areas

The graduate certificate requires the completion of the *Fundamentals* course, and the selection of three other courses chosen from a prescribed list that meet the stated learning objectives. Students will be required to take a course that covers the topics of risk assessment and risk management. Currently, the university offers "Risk Assessment" through the Technology Management Department which will meet this need. In this course, students are exposed to the fundamental tools and operations of assessing risk in a domain-independent environment. Methodologies

examined include, but are not limited to: Preliminary Hazard Analysis, Failure Mode and Effects Analysis, Fault & Event Trees, HAZOP, and Probabilistic Risk Assessment. Another elective course is Advanced Information Assurance offered by the Computer Science Department which exposes students to the seminal literature covering topics such as authentication, access control, and cryptography. This course enables students to have a framework to analyze these issues in the context of their own areas of expertise.

The remaining two elective courses aim to assist the student in bridging the communications gap between the information assurance and cybersecurity professionals and the system operators, technicians, and engineers in critical infrastructure sectors. One course must be a critical infrastructure domain-specific engineering class, such as Resilient Power Systems, Nuclear Safety Systems, or Digital Process Control. These courses are taught in the Electrical Engineering and Mechanical Engineering departments.

Computer Science Master's students could also choose to take a course on Real-time Operating Systems. The goal of this elective group is to provide a deeper dive into the technical and engineering issues related to critical infrastructure resilience.

The final elective course must be a cybersecurity technical elective, such as Computer and Network Forensics, Network Security, or Applied Security Concepts. The intent of the certificate is not to provide a Master's level of subject matter expertise, but rather to provide the ability to foster communications between cybersecurity professionals and various engineering disciplines. While often these courses are considered advanced computer science courses, they focus on a practical approach to modern systems and use available free open source tools that are accessible to the non-computer-science student with some technical aptitude. We have encountered a number of students that have developed information technology skills through personal interest or job experience that are not software engineers. Forensics, for example, has been successfully taught to a number of non-majors with computer savvy that were willing to put in the extra effort to tackle the material and learn the tools and techniques involved.

By completing the sequence of classes for this certificate, students will have tackled the *Fundamentals* course covering the broad range of challenges in critical infrastructure protection, learned the core concepts of risk assessment and management, taken at least one course in an engineering domain-specific topic related to critical infrastructure, and taken at least one course covering technical aspects, tools, and techniques of cybersecurity. As a final requirement of the graduate certificate, students will be required to complete a capstone project that combines the lessons they've learned to approach a topic in a specific critical infrastructure sector.

5 FUTURE WORK

Recognizing that no battle plan survives contact with the enemy, we expect we will need to refine the *Fundamentals* curriculum and the certificate requirements. We plan to elicit feedback not only from students as they progress through the program but from industry partners regarding their need for new employees with skills in infrastructure protection. Armed with this knowledge, we will be able to identify and correct deficiencies, and improve the experience for the students. As part of that improvement effort, we plan to engage the university course coordinators and faculty teaching related courses with an offer to create CIP related content for their courses in the hopes of integrating additional elective courses into the certificate program. The intent is to expand the course base for the certificate without burdening faculty and departments with creating entire new courses.

As the curriculum matures and proves to be worthwhile for students and employers, the university will explore the possibility of expanding the graduate certificate into a master's degree program. As existing classes are augmented to incorporate critical infrastructure resilience and protection topics, the pool of courses from which to draw for inclusion into a master's degree will grow. This will enable the university to select from a more diverse set of courses to provide a program tailored to the students engineering or computer science discipline of choice.

6 CONCLUSION

The efforts to produce a curriculum (including graduate certificate, new course development) at this university covering critical infrastructure protection will not address the entire national need for infrastructure protection professionals. Indeed, one program, let alone one university semester course, cannot supply the protection needs for industry that will expand in the coming years. Our hope is to start the process and help legitimize critical infrastructure protection as a formal field of study. As time passes the discipline will mature and the need for these types of professionals will grow. The university will evaluate and, if warranted, develop a master's degree focused on cross-disciplinary infrastructure protection.

REFERENCES

[1] Collier, Stephen, and Andrew Lackoff. "The Vulnerability of Vital Systems: How 'Critical Infrastructure' Became a Security Problem." *The Politics of Securing the Homeland: Critical Infrastructure, Risk and Securitisation*, 2008: 40-62.

[2] Clinton, William J. "Executive Order 13010 on the President's Commission on Critical Infrastructure Protection (PCCIP)." 1996.

[3] President's Commission on Critical Infrastructure Protection. "Critical Foundations: Protecting America's Infrastructures." https://fas.org/sgp/library/pccip.pdf. (accessed April 5, 2017).

[4] Fisher, Ronald, Mike Norman, and James Peerenboom. "Resilience History and Focus in the United States." in *Urban Disaster Resilience and Security - Novel Approaches for Dealing with Risks in Societies*, edited by Alexander Fekete & Frank Fiedrich. New York: Springer, 2017 (Forthcoming).

[5] Theoharidou, Marianthi, Eleftheria Stougiannou, and Dimitri Gritzalis. "A CBK for information security and critical infrastructure protection." In *Fifth World Conference on Information Security Education*, pp. 49-56. Springer UD, 2007.

[6] Little, Richard G. "Educating the Infrastructure Professional: A New Curriculum for a New Discipline." *Public Works Management & Policy 4*, no. 2 (1999): 93-99.

[7] FEMA – The Emergency Management Institute (EMI) Home Page. https://training.fema.gov/emi.aspx. (accessed April 5, 2017).

[8] Training Available Through ICS-CERT. https://ics-cert.us-cert.gov/Training-Available-Through-ICS- CERT. (accessed April 5, 2017).

[9] Luallen, Matthew E., and Jean-Phillipe Labruyere. "Developing a critical infrastructure and control systems cybersecurity curriculum." In *System Sciences (HICSS), 2013 46th Hawaii International Conference on*, pp. 1782-1791. IEEE, 2013.

[10] Master's Degree Program – Center for Homeland Defense and Security. https://www.chds.us/c/academic-programs/masters-degree-program. (accessed April 5, 2017).

[11] University of Idaho Secure and Dependable Computing Systems Certificate. https://eo.uidaho.edu/sdcs-certificate. (accessed April 5, 2017).

[12] Thomas Morris, Rayford Vaughn, and Yoginder S. Dandass. 2011. A testbed for SCADA control system cybersecurity research and pedagogy. In *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW*

'11), edited by Frederick T. Sheldon, Robert Abercrombie, and Axel Krings. ACM, New York, NY, USA, Article 27.

[13] Critical Infrastructure Higher Education Initiative – Center for Infrastructure Protection &Homeland Security. http://cip.gmu.edu/education-programs/critical-infrastructure-higher-education-initiative/.

[14] Lewis, Ted G. Critical infrastructure protection in homeland security: defending a networked nation. John Wiley & Sons, 2014.

[15] Department of Homeland Security. "NIPP 2013: Partnering for Critical Infrastructure Security and Resilience." https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan- 2013-508.pdf. (accessed April 5, 2017).

[16] Clinton, William. "Presidential Decision Directive 63." The White House, Washington, DC (http://fas.org/irp/offdocs/pdd/pdd-63. htm). (accessed April 5, 2017).

[17] Stouffer, Keith, Joe Falco, and Karen Scarfone. "Guide to industrial control systems (ICS) security." *NIST special publication 800*, no. 82 (2011): 16-16.

[18] Bergmann, Jonathan, and Aaron Sams. Flip your classroom: Reach every student in every class every day. International Society for Technology in Education, 2012.