THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION
AND
HOMELAND SECURITY

NOVEMBER 2014
EDUCATION

VOLUME 14 NUMBER 4

EDITORIAL STAFF

EDITOR
Christie Jones
Dennis Pitman
Tehreem Saifey

PUBLISHER
Melanie Gutmann

Click here to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

Follow us on Twitter here
Like us on Facebook here

This month's issue of *The CIP Report* focuses on **Education**.

First, Christie Jones, Education Program Manager for the Center for Infrastructure Protection and Homeland Security, provides an update on the Critical Infrastructure Higher Education Initiative (CI HEI). Next, a paper submitted by colleagues with the Risk and Infrastructure Science Center at Argonne National Laboratory looks at applying risk-based training to enhance fusion center capabilities. Former Senior Counsel on the House Homeland Security Committee and current Pennsylvania State University Harrisburg professor, Denise Rucker Krepp, discusses teaching critical infrastructure protection (CIP) from a state and local perspective and, finally, Drs. Russell Lundberg and Nathan Jones describe their experience with building an online CIP program at Sam Houston State University.

We would like to take this opportunity to thank this month's contributors. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

The Critical Infrastructure Higher Education Initiative – Resources You Can Use

by Christie Jones

In 2010, the Center for Infrastructure Protection and Homeland Security (CIP/HS) at George Mason University began a partnership with the U.S. Department of Homeland Security's Office of Infrastructure Protection (IP). The objective of their continuing relationship is to support IP's effort to create a comprehensive, unified higher education system that produces and sustains the leaders and workforce required to ensure the security and resilience of the Nation's critical infrastructure. This program, called the Critical Infrastructure Higher Education Initiative (CI HEI), works to develop critical infrastructure educational materials including syllabi, case studies, and technical assistance resources and to make them publicly available to colleges and universities throughout the nation and the world.[1]

To date, CI HEI has created eleven stand-alone critical infrastructure security and resilience (CISR) courses, a five-course CISR certificate program, an eight-course public administration concentration, three supplemental case studies, and two classroom exercises. The CI HEI draws upon subject-matter experts from government, industry, and academia to develop these materials. In addition, course curricula undergo a quarterly review to incorporate changes in policy, literature, and practice as well as feedback received from practitioners and the academic community.

CI HEI courses have been implemented in graduate-level homeland and national security programs across the country. We look to build on this strong academic foundation and increase integration of our CISR courses into a broader range of academic fields at all levels of higher education. The interdisciplinary nature of these resources allow them to be utilized in a variety of disciplines; the CISR concepts illustrated in the curricula make them applicable to emergency management, engineering, environmental sciences, health and health care, business, agriculture, public policy, and law.

George Mason University's Executive MBA - Critical Infrastructure Track program is an excellent example of our efforts to increase engagement with diverse academic programs. Based on the CI HEI five-course certificate program, the EMBA will address the critical areas of risk analysis and management, systems analysis, and cyber security within critical infrastructure sectors. The program emphasizes interagency action and industry-government coordination to achieve business efficiency and resilience.

In response to needs voiced by academics and practitioners in the CISR community, and to facilitate this type of integration in other fields, CI HEI will develop more flexible formats of its current curricula. This year, the *Foundations of CISR* introductory stand-alone course will be broken down into "plug-and-play" modules. These will encapsulate key CISR theories and concepts in easily accessible formats for various disciplines. CI HEI will also create educator packages—fully developed "courses-in-a-box"—to assist faculty and practitioners new to the CISR education space. The "courses-in-a-box" will contain presentations, lesson plans, handouts, and online content that supports implementation of a new CISR foundations course at both the graduate and undergraduate levels. The development of new CISR faculty is another need CI HEI hopes to address with Train-the-Trainer workshops. These workshops will provide potential faculty members with best practices, skills, and tools for teaching CISR courses.

CI HEI will augment these efforts through increased engagement with undergraduate and associate degree programs in various CISR-related disciplines. Many students enter the CISR workforce as undergraduates and often do not pursue advanced

(Continued on Page 3)

[1] All materials can be found at http://cip.gmu.edu/courses/.

(Continued from Page 2)

degrees until well into their careers. With growing interdependency between the public and private sectors in critical infrastructure,[2] students at all levels of higher education must encounter the concepts of security and resilience early on to prepare them to meet the challenges of the ever-changing risk, policy, and operational critical infrastructure environment. CI HEI will target outreach to undergraduate programs, community colleges, and minority-serving institutions through individual institutions and related associations.

As it enters its fourth year, CI HEI remains the vanguard for dissemination of valuable and accessible CISR-related course materials. By responding to the needs of the CISR education community, the initiative is poised to provide academics and practitioners with relevant, timely products and technical assistance. If you have any questions regarding CI HEI, would like to provide feedback, or join our growing list of subject-matter experts, please contact Christie Jones, Education Program Manager, at cjones62@gmu.edu or 703-993-4792. To access CI HEI educational materials please visit http://cip.gmu.edu/courses/. ❖

[2] U.S. Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: U.S. Department of Homeland Security, 2013): 9, available at http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience.

Applying Risk-Based Training to Enhance Fusion Center Capabilities

by Andrea LeStarge, Michael Collins, Janet Ford, Megan Clifford, and Dave Brannegan

Challenge

Both at home and abroad, the United States faces an adaptive enemy in an asymmetric threat environment.[1] To protect the homeland, efforts must concentrate on the timely gathering, receiving, analysis, and dissemination of risk-related information within and among government agencies, private sector owners and operators, and the public. Fusion centers, located in States and major urban areas throughout the country, are instrumental in providing this critical risk-related information, as recognized by the U.S. Department of Homeland Security: "Fusion centers provide multidisciplinary expertise and situational awareness to inform decision making at all levels of government."[2] The National Network of Fusion Centers (NNFC), which is a self-organizing group of fusion centers, "collaborates across jurisdiction and sectors to effectively and efficiently detect, prevent, investigate, and respond to criminal and terrorist activity."[3] The NNFC requires strong analytic support to implement and maintain comprehensive, realistic, high-quality, and actionable risk analysis capabilities. As fusion centers seek to assess local implications of threat information through the use of a formal risk analysis process, the NNFC requires focused support to:

- Eliminate confusion surrounding and demystify the concept of "risk analysis";
- Build confidence amongst the analytic community and prove that most fusion centers already use strong elements of risk analysis on a daily basis; and
- Enhance the overall capability of fusion center analysts to conduct risk analyses and produce associated products that are timely, rigorous, defensible, and useful.

Approach

To address training needs at all levels of government—with specific emphasis on strengthening the critical operational capabilities[4] within fusion centers—the Risk and Infrastructure Science Center (RISC) within the Global Security Sciences Division at Argonne National Laboratory designs, develops, and delivers risk-based training courses to state and local fusion center analysts and homeland security stakeholders.

These courses leverage RISC expertise in risk assessment to evaluate security and resilience of U.S. critical infrastructure threatened with disruption as a result of natural hazards, accidents, or deliberate acts such as terrorist attacks.[5] Whether utilizing probable scenarios of concern or actual threat information received from various sources, RISC incorporates physical and cyber security analysis, databases and tools, modeling, and simulation technologies to assess

(Continued on Page 5)

[1] U.S. Department of Homeland Security, *State and Major Urban Area Fusion Centers* (Washington, D.C., July, 2012), accessed October 24, 2014. http://www.dhs.gov/sites/default/files/publications/Fusion%20Centers%20Handout.pdf.
[2] Ibid.
[3] Ibid.
[4] In partnership with the federal government, fusion centers have distilled the various priorities of their missions into four critical operational capabilities (COCs): 1. **Receive**: ability to receive classified and unclassified information from Federal partners; 2. **Analyze**: ability to assess local implications of threat information through the use of a formal risk assessment process; 3. **Disseminate**: ability to further disseminate threat information to other State, local, tribal, territorial, and private sector entities within the fusion center's area of responsibility; and 4. **Gather**: ability to gather locally generated information and then to aggregate, analyze, and share it with Federal partners, as appropriate. Source: U.S. Department of Homeland Security, *State and Major Urban Area Fusion Centers* (Washington, D.C., July, 2012) accessed October 29, 2014. http://www.dhs.gov/sites/default/files/publications/Fusion%20Centers%20Handout.pdf.
[5] Argonne National Laboratory, "Decision and Information Sciences: Infrastructure Assurance," accessed October 29, 2014. http://www.dis.anl.gov/exp/ia/index.html.

(Continued from Page 4)

vulnerabilities, resilience, and consequences. The resulting training enhances risk assessment capabilities while emphasizing the strategic and tactical responsibilities of fusion center analysts. The introductory and intermediate risk-related courses are described below.[6]

Introduction to Risk Analysis for Fusion Center Analysts

As fusion center analysts seek to assess the local implications of threat information through the use of a formal risk analysis process, needs for training are identified. In particular, education is necessary to eliminate the confusion surrounding and demystify the concept of "risk analysis"; build confidence among those in the analytic community by proving that most fusion centers already use strong elements of risk analysis on a daily basis; and enhance the overall capability of fusion center analysts to conduct risk analyses and produce associated products that are timely, rigorous, defensible, and useful.

The three-day *Introduction to Risk Analysis for Fusion Center Analysts* course clarifies the concept of risk, builds confidence among the analysts, and allows analysts to implement a repeatable risk analysis process using their own intimate knowledge of their area of responsibility (AOR). Separate modules introduce the core elements of the risk equation—threat, vulnerability, and consequence—and an exercise on each element follows. Supporting modules present other analytic topics, including the use of scales and an introduction to infrastructure dependencies as a "risk multiplier." The final, capstone exercise in the *Introduction to Risk Analysis* course brings the individual, core element analyses of threat, vulnerability, and consequence together into an integrated risk product that highlights options for consideration to bolster, sustain, or enhance resilience; the students then have an opportunity to brief their group's results. This course strengthens student understanding of the role and importance of risk analysis; helps to ensure that students will produce consistent, quality, and defensible analytic products; and, ultimately, provides a foundation for advanced training in specific risk analysis techniques.

Intermediate Risk Analysis for Fusion Center Analysts

Building on the foundation established in the introductory training and integrating various all-source analyses, the *Intermediate Risk Analysis for Fusion Center Analysts* course delves deeper into risk analysis resources, methods, and tools. In particular, the course concentrates on a critical fusion center role, developing analytic products for senior leadership that provide tactical, risk-informed recommendations. Simulating this responsibility, students are given the task of writing a risk assessment for a national-level special event held in their AOR and presenting each section of the assessment to the class. Students are challenged to develop a defensible risk product under very realistic time and data constraints, with the goal being to develop a product within an 8-hour period. The course is designed to allow analysts to practice the application of their risk analysis skills to better prepare them for the pressures associated with a realistic fusion center analytic task.

Using a simple risk analysis framework, RISC trainers seek to leverage the unique expertise (based on the analysts' intimate knowledge of their AORs) of critical infrastructure and intelligence analysts in a consistent, focused, and repeatable process.

Using the risk formula established in the introductory course, students in the *Intermediate Risk* course analyze local and national threat information and identify the most probable scenarios of concern for the fictional special event and associated venues. Once these threats are identified, students continue with the risk analysis framework and determine the probability of success given those attacks (vulnerability assessment) and the potential impact of those attacks (consequence assessment). Students conclude their risk analyses by developing options for consideration for threat mitigation and overall risk reduction. The curriculum includes a review of sample fusion center risk products

(Continued on Page 6)

[6] For the time being, although Argonne has defined the elements that should constitute an advance risk course, this course is not offered yet.

(Continued from Page 5)

to highlight best practices and lessons learned while supporting peer-to-peer exchanges. By the end of this course, each participant has the appropriate training, tools, and mentoring to develop a sample fusion center risk product, with ample opportunity to receive instructor and peer feedback.

Benefits

Fusion center analysts require defensible, comprehensive, and actionable risk-analytic processes to apply under extremely aggressive production timelines, all while executing critical capabilities aimed at information sharing to protect the homeland. As evidenced by post-course surveys and ongoing support provided to students, graduates of RISC classes have applied the key learning objectives in their daily roles as analysts, and, as a result, they are producing strong, defensible, and repeatable risk analytic products. Through the development of risk assessments, analysts are contributing to all aspects of the intelligence cycle; supporting risk-reduction efforts taken by federal, state, local, and private sector partners; and informing risk management activities (e.g., the allocation of resources to mitigate threats) on those very same strategic and tactical levels. These products demonstrate the effectiveness of the training and the direct contribution that the training has made toward enhancing fusion center capabilities nationwide. Developing and applying additional training, whether for fusion centers or other stakeholders, may also prove beneficial to enhance capabilities promoting the security and resilience of the nation.

Acknowledgment

The submitted manuscript has been created by UChicago Argonne, LLC, Operator of Argonne National Laboratory ("Argonne"). Argonne, a U.S. Department of Energy Office of Science laboratory, is operated under Contract No. DE-AC02-06CH11357. The U.S. Government retains for itself, and others acting on its behalf, a paid-up nonexclusive, irrevocable worldwide license in said article to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government. The development of the courses described in this paper has been funded by the U.S. Department of Homeland Security Protective Security Coordination Division under Contract No HSHXDC-13-X-00223.

Andrea LeStarge, Michael Collins, Janet Ford, Megan Clifford, and Dave Brannegan are with the Risk and Infrastructure Sciences Center, Global Security Sciences Division, Argonne National Laboratory. Mr. Brannegan is the Director of the Infrastructure Assurance Center, while Ms. Clifford serves as Deputy Director. Both Ms. LeStarge and Ms. Ford serve as Risk Analysts and Mr. Collins is an Infrastructure and Preparedness Specialist. ❖

Ebola Response: Case Study for Critical Infrastructure Protection Students

By Denise Rucker Krepp

Critical infrastructure protection (CIP) is traditionally taught from the federal perspective. The federal government writes the laws and develops the national policies. At Penn State Harrisburg, students are using the recent Ebola outbreak to learn about CIP from the state and local perspective. The goal is to better educate students on the role state and local officials have in influencing and implementing CIP policies.

Federal laws such as the Homeland Security Act, the Intelligence Reform and Terrorism Prevention Act, and the Implementing Recommendations of the 9/11 Commission Act are written by Congress and signed into law by the President. Executive-level departments like the Department of Homeland Security are tasked with implementing the congressionally mandated policies and regulations.

Similarly, the federal government is responsible for drafting national strategies. The national strategy for CIP is the National Infrastructure Protection Plan.[1] The NIPP outlines the sixteen critical sectors, the departments responsible for overseeing protective measures, and the federal government's strategy to work with state and local authorities to protect these sectors.

Significant attention has been focused on the healthcare field this fall because of the Ebola outbreak, especially after the first confirmed case in the United States appeared in a Dallas hospital in September. Pursuant to the NIPP, the Secretary of Health and Human Services (HHS) is responsible for the Healthcare and Public Health Sector. According to the most recent Healthcare and Public Health Sector-Specific Plan,[2] the Secretary delegated this authority to the Assistant Secretary for Preparedness and Response. The 2010 plan's vision is to "achieve overall resilience against all hazards." The plan includes pandemics, like Ebola, in its definition of all hazards.

Penn State Harrisburg students in the masters level critical infrastructure protection class are examining whether or not state and local officials followed the NIPP and SSP guidelines when responding to the outbreak. At the strategic level, did governors contact HHS before developing state quarantine policies? If so, what recommendations (and limitations) did HHS provide and did the governors accept this guidance? At the tactical level, was the Dallas hospital prepared to treat Ebola patients? Given that four years have elapsed since the SSP was published, had the Dallas hospital taken adequate measures to make sure that it was compliant with the SSP?

The students learn that they cannot assume that state and local authorities must or will follow federal strategies. Governor Chris Christie's decision to impose a mandatory 21-day quarantine in New Jersey differed from the guidance put out by the Centers for Disease Control and Prevention (CDC). Students also become familiar with the state authorities that gave Governor Christie the authority to issue the order. They are also analyzing the relationship between this order and the CDC guidance. Specifically, they are examining when state governors can take action that is greater than that recommended by the federal government.

Penn State Harrisburg students are

(Continued on Page 8)

[1] U.S. Department of Homeland Security, NIPP 2013: Partnering for Critical Infrastructure Security and Resilience (Washington, D.C.: U.S. Department of Homeland Security, 2013), available at http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf.

[2] U.S. Department of Health and Human Services, Healthcare and Public Health Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan (Washington, D.C.: U.S. Department of Health and Human Services, 2010), available at http://www.dhs.gov/xlibrary/assets/nipp-ssp-healthcare-and-public-health-2010.pdf.

(Continued from Page 7)

also learning about the factors that motivate a governor to act. For instance, Governor Andrew Cuomo of New York originally issued a quarantine order that was similar to that issued by Governor Christie, but later modified his order to allow isolation at home, as detailed in an article by *The New York Times*.[3] Using this article as a source document, students are learning about what motivates state officials to act urgently, how federal officials can work with state officials to modify an original state order, and why state officials may be influenced by federal officials and other groups.

Additionally, students examine how actions taken by state officials like Governor Christie can impact federal strategies like the NIPP. The current NIPP assumes that everyone—federal, state, and local authorities—will implement the same prevention, response, and recovery measures. The actions taken by Governors Cuomo and Christie are one demonstration of how that assumption is false.

I believe updating the NIPP to close the gap between state actions and federal policy will be a priority over the next couple of years. The federal government does not want state officials to take measures that conflict with federal strategies. Resolving conflicts however can take significant time, something authorities do not have when trying to successfully respond to an incident.

Students are asked to put on their federal cap and think about steps the government can take to improve the NIPP and state compliance. Likewise, students are asked to put on their state cap and think about ways states can use recent Ebola responses to improve the NIPP. Why did the states and local authorities not rely on the Healthcare SSP when the Ebola outbreak began? What additional measures do the states want the federal government to take that will satisfy state-specific concerns? What are the lessons learned that can be used to update the NIPP and SSP?

The federal government wrote the NIPP, but state and local authorities do not have to implement it. This lesson has been very eye-opening to students, many of whom work for the federal government. They assumed that state action would follow federal action, which has not proven to be the case with the Ebola outbreak. Learning about how state officials view federal strategies like the NIPP has helped them better understand the role of states in carrying out these strategies. When an emergency arises, state and local assets will the first ones on scene, and they cannot be taken for granted.❖

[3] Matt Flegenheimer, Michael D. Shear, & Michael Barbaro, "Under Pressure, Cuomo Says Ebola Quarantines Can Be Spent at Home," *New York Times*, Oct. 26, 2014, available at http://www.nytimes.com/2014/10/27/nyregion/ebola-quarantine.html?_r=0.

Building an Online CIP Program at Sam Houston State University: Finding an Institutionally Cooperative Eco-System

by Russell Lundberg and Nathan Jones

Sam Houston State University has recently established an online CIP-certificate program at the graduate level. In developing the requisite courses, we found an incredibly cooperative and supportive ecosystem around critical infrastructure protection that fosters the development of new programs. We were able to draw on this community as well as the resources and strong reputation of the University's criminal justice program to develop courses for mid-career professionals in law enforcement and homeland security. It is our hope that this article will serve as a partial guide to other University programs making the foray into online education in critical infrastructure protection.

Recognizing the Need for Critical Infrastructure Protection Education

The Department of Security Studies at Sam Houston State University is part of the College of Criminal Justice. SHSU has been providing education and training to law enforcement agencies for more than fifty years and its criminal justice program is one of the nation's premier programs. Besides traditional undergraduate and graduate courses, SHSU provides continuing education for practitioners and officials through its close association with the Law Enforcement Management Institute of Texas (LEMIT) and the Correctional Management Institute of Texas (CMIT).

The Department of Security Studies is a more recent addition to the SHSU College of Criminal Justice. As is typical of homeland security programs, the need for education in security was recognized in the years following the events of September 11, 2001. According to Dr. Jurg Gerber, acting chair of the department, "The events of 9/11 forced criminal justice practitioners to rethink their work. While street crime and white collar crime had always been important, 9/11 emphasized the need to include homeland security."[1] A Master of Science in Security Studies was introduced in 2006, designed for students with baccalaureate degrees in criminal justice, political science, or related disciplines who were seeking employment in private and government security. This degree was offered face-to-face, with the number of students increasing to approximately twenty students per year. During the summer of 2014, the master's degree was retooled and renamed a Master of Science in Homeland Security Studies. Part of this reorganization was the addition of two new certificates in emergency management and in critical infrastructure protection and creation of an option for online education.

The decisions to make critical infrastructure courses and to offer them online were made at the same time. The College of Criminal Justice already had several online degrees, including both bachelor and master degrees. The preexisting online classes were a particularly useful bridge between the educational content of the university and the training of LEMIT and CMIT; the online certificate and degrees provide an opportunity for mid-career law enforcement management to advance their careers while still working full-time. One member of the Security Studies faculty, Dr. Magdalena Denham, had trained countless law enforcement officers over the years at LEMIT and had always included aspects of systemic cascading failure as part of incident-command simulation training. From this experience it was believed that a natural direction for law enforcement captains and chiefs would be to move to state or national positions, and education in homeland security would be a desired step-up. The

(Continued on Page 10)

[1] Trey Cawley, "New Homeland Security Studies Program Debuts," *CJ Blog* (August 13, 2014), available at http://shsucj.blogspot.com/2014/08/new-homeland-security-studies-program.html.

(Continued from Page 9)

college was enthusiastic about the prospect based on their experience with online degrees in criminal justice, and three new courses in critical infrastructure were approved for online delivery. The approval process was not necessarily easy—the approval timeline did present challenges for advertising the courses—but with the strong support of the college and university the programs were underway.

Creating Online Classes in a Supportive Environment

With the groundwork for the CIP online program laid, the specific courses needed to be developed. As new faculty with relevant experience, we were given the task of building these new critical infrastructure courses. We immediately found a highly cooperative ecosystem that fostered the sharing of information and the open distribution of educational materials, with three centers being particularly useful. George Mason University's Center for Infrastructure Protection and Homeland Security maintains updated syllabi for CIP courses. The Naval Postgraduate School's Center for Homeland Defense and Security maintains the University Agency Partnership Initiative which also provides myriad resources for CIP education and more importantly a forum for the exchange of information between CIP practitioners and academics.[2] The Texas A&M Engineering Extension Service (TEEX) offered numerous in-person CIP courses which we were able to take advantage of, both to learn more about the state of the art and to network with practitioners on the development of our courses.[3]

All of these amazing resources are a function not only of the hard work and passion of the people behind them, but also the support and environment created by the Department of Homeland Security through the funding of academic centers of excellence and other initiatives. This cooperative ecosystem extended to personal relationships with the professors and practitioners we reached out to in the process of developing syllabi. We found that academics and practitioners across the field were generous with their time and expertise. Professor James Phelps of Angelo State University was particularly helpful, as was Lieutenant Colonel Steve Hart of the U.S. Military Academy (West Point), who allowed us to pick his brain and pointed us to educational resources in the open-source domain.

Within this cooperative environment, we wanted to make certain our curriculum and program was uniquely ours and played to the competitive advantages of Sam Houston State University. Geographically, SHSU is well positioned to address energy and port security issues, and its proximity to the world-renowned Texas Medical Center puts us in a good position to focus on the future of public health security, an area more people are paying attention to in the midst of the current Ebola crisis. Additionally, the strength of our criminal justice program provided extensive access to local, state, and federal law enforcement officials to help us identify practitioner concerns.

Given our educational backgrounds, with dissertations on risk management[4] and resilience in organized crime networks,[5] we chose to focus on resilience as a key theme in our course curricula. Our courses included two courses in CIP and CIP Risk Management (which have been developed) and one in cybersecurity (still under development). The critical infrastructure protection course included roughly 20% risk management concepts and network theoretic concepts and focused the rest of its efforts on the substantive areas of CIP, such as key themes in current CIP government structures

(Continued on Page 11)

---

[2] "Center for Homeland Defense & Security," *The Naval Postgraduate School & the U.S. Department of Homeland Security: Center for Homeland Defense and Security*, accessed October 31, 2014, http://www.chds.us/?home; "Homeland Security Educators: The University and Agency Partnership Initiative," accessed October 31, 2014, http://www.uapi.us/.

[3] "TEEX Security & Infrastructure Protection," accessed October 31, 2014, http://www.teex.org/teex.cfm?pageid=PublicSafetyprog&area=PublicSafety&templateid=1775.

[4] Russell Lundberg, "Comparing Homeland Security Risks Using a Deliberative Risk Ranking Methodology" (Dissertation, RAND Pardee School, 2013), http://www.rand.org/pubs/rgs_dissertations/RGSD319.html.

[5] Nathan Jones, "The State Reaction: A Theory of Illicit Network Resilience" (Dissertation, University of California, Irvine, 2011).

(Continued from Page 10)

like partnerships, and introductions to some of the CIP sector specific issues under these themes. The risk management course focused primarily on more elevated risk management concepts, threat and risk assessments and their implementation, and higher level methodologies, such as game theory and fault-tree analysis.

In developing the courses, something amazing happened. The very students we would teach reached out to us. As practitioners seeking to advance their careers through the pursuit of master's degrees related to CIP, this presented an amazing resource at our disposal. TEEX instructors such as Debi Harris, who would join our program, gave us valuable feedback proving that whereas online classes may lack a certain level of personal interaction due to limited face-to-face contact, they facilitate the involvement by practitioners who supplement the experiences by bringing their knowledge to class discussion boards.

Contact with our future students also gave us feedback on what would and would not be possible in the online environment. We immediately had to make decisions about synchronous versus asynchronous classes. Would the classes be held at fixed times with student and faculty interaction or would they be designed so the students could work on their own schedules? Feedback from employed practitioners made it clear that full synchronicity was not viable. We also thought of students in the military on foreign deployments who might not be able to attend synchronous courses. We decided on a middle course that primarily employs an asynchronous format but includes two or three synchronous sessions throughout the semester—in part designed to test their viability and the technical platform (Blackboard).

Another difference between the online and face-to-face courses is the ability to apply the materials to real-world applications. The university encourages Academic Community Engagement (ACE) in its courses, described as "a teaching method that combines community engagement with academic instruction." There are opportunities in the face-to-face course for group projects applying tools of risk management to needy organizations, starting with the university but later to be extended to non-profit and governmental organizations in the area. These risk assessment and management exercises require substantial effort, and in the face-to-face course this meant group projects. This kind of group coordination will be more difficult for the online course, particularly for projects related to a specific location, and it is not clear that students will be able to perform these sorts of exercises on their own. If and how the online course can integrate ACE is still being explored.

Moving Forward

Now that the courses have been created, it is time to teach them. *Critical Infrastructure Protection* will be offered online in the spring. While the standard sequence of the online master's degree will have the critical infrastructure courses offered in the second year, with *Critical Infrastructure Protection* in the fall and *Critical Infrastructure Risk Management* in the summer, courses are being offered out of sequence for students interested only in the certificate and not the master's degree. Certain adjustments will need to be made such as finding alternatives for synchronous group exercises and conducting community engagement but education is a process and not only a result. A class is never one way, and we learn from our students at the same time they learn from us. We look forward to the journey.

References:

Cawley, Trey. "New Homeland Security Studies Program Debuts." CJ Blog, August 13, 2014. http://shsucj.blogspot.com/2014/08/new-homeland-security-studies-program.html.

"Center for Homeland Defense & Security." The Naval Postgraduate School & the U.S. Department of Homeland Security: Center for Homeland Defense and Security. Accessed October 31, 2014. http://www.chds.us/?home.

"Homeland Security Educators: The University and Agency Partnership Initiative." Accessed October 31, 2014. http://www.uapi.us/.

Jones, Nathan. "The State Reaction: A Theory of Illicit Network Resilience." Dissertation, University of California, Irvine, 2011.

(Continued on Page 12)

(Continued from Page 11)

Lundberg, Russell. "Comparing Homeland Security Risks Using a Deliberative Risk Ranking Methodology." Dissertation, RAND Pardee School, 2013. http://www.rand.org/pubs/rgs_dissertations/RGSD319.html.

"TEEX Security & Infrastructure Protection." Accessed October 31, 2014. http://www.teex.org/teex.cfm?pageid=PublicSafetyprog&area=PublicSafety&templateid=1775.

Dr. Nathan Jones is an Assistant Professor with Sam Houston State University's Department of Security Studies. Prior to joining the department, Dr. Jones was the Alfred C. Glassell III Postdoctoral Fellow in Drug Policy at Rice University's Baker Institute for public policy, where his research focused on drug violence in Mexico. He has published with numerous think tanks, including the Woodrow Wilson International Center for Scholars, the Center for Strategic and International Studies, and InSight Crime.

Dr. Russell Lundberg is an Assistant Professor with Sam Houston State University's Department of Security Studies. Before joining the department, Dr. Lundberg served as an assistant policy analyst at the RAND Corporation, a nonprofit institution that helps improve policy and decision making through research and analysis. He worked on projects in homeland security, exploring methods for improving risk assessments, and projects on aviation security, postal security, and law enforcement intelligence. ❖

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1