Homeland Security Academic Advisory Council

Member Briefing Materials

March 19, 2014

Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Homeland Security Academic Advisory Council (HSAAC) Meeting Agenda

Wednesday, March 19, 2014
Ronald Reagan Building, Room B 1.5-10 (Floor B1)
1300 Pennsylvania Avenue, N.W.

10:00 a.m.	Call to Order
10:02 a.m.	Opening Remarks, Introductions and Overview of the Day
10:15 a.m.	HSAAC Member Roundtable
10:45 a.m.	Ex-Officio Member Remarks and Discussion
11:15 a.m.	International Students Subcommittee Report and Discussion
11:35 a.m.	Cybersecurity Subcommittee Report and Discussion
12:00 p.m.	Lunch
12:30 p.m.	DHS Response to Council Progress
1:00 p.m.	Update on DHS Campus Resilience Pilot Program
1:20 p.m.	Campus Resilience Subcommittee Report and Discussion
1:40 p.m.	Additional Subcommittee Reports and Discussion
2:40 p.m.	Public Comment Period*
3:10 p.m.	Council Votes on Potential Recommendations
3:30 p.m.	Adjourn

** Please note that the meeting may close early if the Council has completed its business. Public comment period times are subject to change.*

2014-03-14

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Subcommittees of the Homeland Security Academic Advisory Council

1. **Subcommittee on Student and Recent Graduate Recruitment**
    1. How to attract student interns, student veterans, and recent graduates to jobs at DHS;
    2. How to use social media and other means of communication to most effectively reach this audience; and
    3. How to ensure that students and recent graduates of Historically Black Colleges and Universities, Hispanic Serving Institutions, Tribal Colleges and Universities, and other Minority Serving Institutions know of and take advantage of DHS internship and job opportunities.

2. **Subcommittee on Homeland Security Academic Programs**
    1. How to define the core elements of a homeland security degree at the associate's, bachelor's and master's levels;
    2. How to apply the TSA Associates Program model to other segments of the DHS workforce who wish to pursue a community college pathway;
    3. How to form relationships with 4-year schools so that DHS employees' credits transfer towards a higher level degree;
    4. How to enhance existing relationships between FEMA's Emergency Management Institute and the higher education community to support Presidential Policy Directive 8 (PPD-8), expand national capability, and support a whole community approach;
    5. How to expand DHS cooperation with the Department of Defense academies and schools to provide DHS' current employees with educational opportunities;
    6. How colleges and universities might offer academic credit for DHS training; and
    7. How to better promote degree and certificate programs to DHS employees who are seeking professional development.

3. **Subcommittee on Academic Research and Faculty Exchange**
    1. How academic research can address DHS' biggest challenges;
    2. How DHS operational Components can form lasting relationships with universities to incorporate scientific findings and R&D into DHS' operations and thought processes;
    3. How universities can effectively communicate to DHS emerging scientific findings and technologies that will make DHS operations more effective and efficient;
    4. How we can jointly create a robust staff/faculty exchange program between academe and DHS; and
    5. How DHS assesses the risk and value of its major programs.

4. **Subcommittee on International Students**
    1. How DHS can improve its international student processes and outreach efforts;
    2. How DHS can better communicate its regulatory interpretations, policies and procedures to the academic community; and
    3. How DHS can accommodate and support emerging trends in international education.

5. **Subcommittee on Campus Resilience**
    1. How colleges and universities use specific capabilities, tools, and processes to enhance campus and community resilience as well as the cyber and physical infrastructure;
    2. How DHS' grant programs may be adjusted to support resilience-related planning and improvements;
    3. How campuses can better integrate with community planning and response entities;
    4. How to implement the whole community approach and preparedness culture within student and neighboring communities;
    5. How to strengthen ties between DHS' Federal Law Enforcement Training Center and campus law enforcement professionals; and

6. How DHS can better coordinate with individual campus information technology departments on the risks towards and attacks on computer systems and networks.

6. <u>Subcommittee on Cybersecurity</u>

1. How to attract students, student veterans and recent graduates to cybersecurity jobs at DHS;
2. How DHS can better promote the DHS/ National Security Agency National Centers of Academic Excellence cybersecurity programs to the higher education community;
3. How to define the core elements of cybersecurity degree and certificate programs to prepare graduates for mission-critical cyber jobs at DHS;
4. How DHS can facilitate and strengthen strategic partnerships with industry, national labs, colleges, universities and others to build the cybersecurity workforce;
5. How DHS can partner with academia to build a pipeline of diverse students in Science, Technology, Engineering and Math (STEM); and
6. How key subcategories in cybersecurity – such as policy, critical infrastructure, human factors, intellectual property, and others – can inform academic pathways to meet national needs.

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland Security Academic Advisory Council

Chair:
Dr. Wallace D. Loh

Members:
Dr. Joseph E. Aoun
Dr. Lezli Baskerville
Ms. Carrie L. Billy
Dr. Walter G. Bumphus
Dr. David M. Dooley
Dr. Royce C. Engstrom
Dr. Antonio R. Flores
Dr. Rufus Glasper
Dr. Jay Gogue
Ms. Marlene M. Johnson
Dr. Eric W. Kaler
Dr. R. Bowen Loftin
Dr. Gail O. Mellow
Hon. Ruby G. Moy
Dr. Mohammad Qayoumi
Dr. John Sexton
Rear Admiral Sandra Stosz
Dr. Dianne Boardley Suber

January 13, 2014

The Honorable Jeh Charles Johnson
Secretary of the U.S. Department of Homeland Security
Washington, DC 20528

Dear Mr. Secretary:

At the March 20, 2013 meeting of the Homeland Security Academic Advisory Council (HSAAC), Secretary Napolitano tasked us with forming a subcommittee on cybersecurity, chaired by San José State University President Mohammad Qayoumi, to provide advice and recommendations on DHS' cybersecurity recruitment and workforce education efforts.

The subcommittee on cybersecurity met multiple times via teleconference between May and June to develop draft recommendations for approval by the full HSAAC. At its July 17, 2013 meeting, the HSAAC voted to approve a total of 16 draft recommendations.

I. Subcommittee on Cybersecurity

Cyber intrusions and attacks have increased dramatically over the last decade, and the landscape of cyber threats is constantly evolving. To ensure a stable, safe, and resilient cyberspace, it is vital to develop and attract top cyber talent and highly qualified candidates to DHS.

In order to build a sustainable pipeline of talent, it is important to create pathways for students to become and stay engaged in cybersecurity throughout their education. Students within underserved and veteran communities represent an important demographic that DHS should target. DHS is actively working to create cybersecurity educational and employment opportunities for students and student veterans, through efforts such as the sponsorship of cyber competitions. As community colleges are well-positioned to develop a large number of highly skilled cybersecurity professionals, DHS should explore and expand innovative partnerships with these institutions.

Based on these findings the Subcommittee on Cybersecurity recommends:

1. DHS should continue hosting monthly tours of DHS' National Cybersecurity and Communications Integration Center (NCCIC) for secondary, post-secondary and veteran students involved in cybersecurity and other STEM disciplines. DHS should arrange virtual tours of the NCCIC to accommodate students located outside of the National Capital Region.

2. DHS should promote and support cyber-related educational and career opportunities to engage students at the start of their formal education, beginning at the primary level and continuing through the middle school, secondary and postsecondary levels, in cybersecurity and other STEM disciplines. These efforts should include support of community college-based programs that provide hands-on, technical cybersecurity training and education.

3. DHS should compile a list of cyber competitions, including any measures of program success (i.e. amount of private sector dollars contributed, number of participants, and number of job offers extended to participants), to assess the return on investment and target proven programs to invest in and support.

4. DHS should establish analytics and/or a tracking program to gather data on the post-activities of students involved in cyber camps and other cyber programs, to determine ways to continually engage these students and encourage their entry into cyber careers.

    a. DHS should track the succession of students from 2-year cyber-related degree programs to 4-year cyber-related degree programs and/or careers.

5. DHS should target outreach efforts at underserved communities to improve their pathways to cyber-related educational and career opportunities.

    a. DHS should target outreach to women, people of color, and underserved communities to promote cybersecurity clubs/camps with an emphasis on individual and team-oriented projects as well as the growing impact of cybersecurity in our technologically integrated world. An emphasis on these aspects of cybersecurity and its social benefits will broaden the appeal of these clubs/camps.

6. DHS should partner with the Departments of Veterans Affairs (VA) and Defense to inform veterans and transitioning service members of how to use the College Level Examination Program (CLEP) to obtain credit for active duty experience and academic work while in service.

7. DHS should partner with VA to enhance awareness of existing road mapping tools such as VA for Vets and MyCareer@VA, as well as incorporate DHS employment opportunities in such tools.

8. DHS should identify and leverage existing college and university cyber boot camps for ROTC cadets as a model for student veterans.

9. DHS should foster the growth of the U.S. Coast Guard Academy's (CGA) cyber-related educational opportunities and programs:

    a. Examine the feasibility of CGA applying as a DHS/National Security Agency Center for Academic Excellence in Information Assurance/Cyber Defense.

    b. Partner with CGA on DHS' cyber-related initiatives, utilizing CGA as a test-bed for pilot programs.

    c. Establish an internship program for CGA cadets, modeled after the Secretary's Honors Program Cyber Student Volunteer Initiative.

10. DHS should develop reciprocal partnerships with private companies to create an 'exchange program' for DHS employees and interns, in order to broaden the experience of entry-level cybersecurity professionals.

11. DHS should expand the National Initiative for Cybersecurity Careers and Studies website to include a comprehensive and interactive asset map of government cyber programs, careers, and educational and training resources.

12. DHS should establish and support a Department-wide social media and outreach strategy directed at its cyber-related programs, initiatives and opportunities. The strategy should incorporate input from academic associations, students, faculty, and other higher education sources, and should target students, student veterans and recent graduates interested in cyber-related careers.

These recommendations are the culmination of many months of work and could not have been possible without the support of the DHS Office of Academic Engagement and many DHS subject matter experts. The HSAAC urges DHS to consider these recommendations for implementation.

At our upcoming full HSAAC meeting on March 19, 2014, we anticipate deliberation and action on additional recommendations from each of the six subcommittees.

Sincerely,

Wallace D. Loh

Dr. Wallace Loh
Chair, HSAAC

David Adams
Senior Policy Advisor for Law Enforcement
U.S. Department of Justice

David Adams serves as a Senior Policy Advisor for Law Enforcement for the Bureau of Justice Assistance (BJA) where his main areas of responsibility include Campus Safety and Crime Prevention.

Prior to joining BJA, Adams served in the Virginia Office of the Attorney General as Executive Director of the Attorney General's Task Force on Access to Higher Education, and as Director of Programs where Adams was responsible for oversight of the Office's efforts to combat domestic violence, the TRIAD Program – a program designed to protect senior citizens from scam artists and telemarketing fraud – and working with victims of violent crime through the Victim Notification Program.

Prior to his appointment to the Office of the Attorney General, Adams was appointed Assistant Secretary of Education by Virginia Governor Jim Gilmore, where his duties included legislative liaison and policy advisor. He was later appointed Deputy Secretary for Higher Education where he was responsible for oversight of the Commonwealth's 23 community colleges and 15 public colleges and universities.

Adams is a cum laude graduate of the University of Richmond where he earned his Bachelor Degree.

David Esquith
Director, Office of Safe and Healthy Students
U.S. Department of Education

David Esquith is the Director of the U.S. Department of Education's Office of Safe and Healthy Students located within the Office of Elementary and Secondary Education.

Esquith is a former Peace Corps volunteer, special education teacher, lobbyist for the Association for Retarded Citizens, and Congressional aide.

Before coming to the Office of Safe and Healthy Students, he worked in the U.S. Department of Education's Office of Special Education and Rehabilitative Services.

Edward J. Ramotowski
Deputy Assistant Secretary for Visa Services
U.S. Department of State

Edward Ramotowski assumed his current position as Deputy Assistant Secretary for Visa Services at the U.S. Department of State in July 2012. In that position he oversees the Visa Office in Washington DC, two domestic processing centers, as well as visa operations at over 200 U.S. Embassies and Consulates abroad.

From August 2006 to July 2009 he served as Principal Officer at the U.S. Consulate General in Guadalajara, Mexico, followed by three years as Managing Director for Visa Services. He has previously worked as Special Assistant to the Assistant Secretary of State for Consular Affairs, Chief of the Consular Section at the U.S. Embassy in Nassau, Bahamas and as U.S. Consul in Warsaw, Poland. Other tours of duty have included service as a consular and political officer in Bogota, Colombia and consular officer in Kingston Jamaica.

Ramotowski has also served in Washington as a country officer in the Office of Andean Affairs, as well as a watch officer in the State Department Operations Center and on the White House Situation Room staff. He has received several Department of State Superior Honor and Meritorious Honor Awards, and in 2000 was recognized with the Barbara Watson Award for consular excellence.

Ramotowski joined the Foreign Service in 1986. He is a graduate of Georgetown University and the National War College. He is married to Foreign Service officer Jemile Bertot, and they have two children.

Progress Report from the Homeland Security Academic Advisory Council's Subcommittee on International Students

The Subcommittee on International Students is charged with providing advice and recommendations to the Secretary and senior leadership on the following:

1. ***How DHS can improve its international student processes and outreach efforts;***

2. *How we can better communicate our regulatory interpretations, policies and procedures to the academic community; and*

3. *How we can accommodate and support emerging trends in international education.*

Co-Chaired by Association of International Educators (NAFSA) Executive Director and CEO Ms. Marlene M. Johnson and New York University President Dr. John Sexton, the subcommittee met via teleconference on January 28 and February 11, discussing tasking 1 (in bold font, above) as well as potential recommendations.

Overall Findings

- U.S. Customs and Border Protection (CBP) provides its Officers with extensive training through its Officer Basic Training Program, including classroom and scenario based training on a number of topics including immigration law and, specifically, international students. Additional training is provided following deployment, including a two-hour course on the Student and Exchange Visitor Information System (SEVIS) and international student document requirements.

- CBP does not publicize its internal policies and procedures that provide operational guidance on the entry process and decisions made by CBP Officers at ports of entry. The non-law enforcement sensitive portions of CBP's internal policies and procedures could serve as a useful guide for travelers, including international students, as they prepare to travel to the United States.

- DHS maintains numerous customer service initiatives and programs to support international students and staff at U.S. institutions in understanding and navigating policies and processes. Promotion of these initiatives and programs will increase the public's understanding of DHS resources and promote compliance with DHS policies.

- The U.S. Immigration and Customs Enforcement (ICE) Student and Exchange Visitor Program (SEVP) has made significant progress in reducing its school certification processing times and increasing engagement with stakeholders. ICE SEVP staff increases are needed to implement ongoing initiatives such as the modernization of the Student and Exchange Visitor Information System (SEVIS).

Draft Recommendations

The Subcommittee on International Students makes the following draft recommendations:

1. DHS should incorporate international student-specific modules into training for new and continuing employees of DHS components and agencies with a role in the international student process.

2. CBP should publicize the non-law enforcement sensitive policies and procedures related to international student entry to increase transparency and understanding of the operational procedures that guide CBP Officers in the entry process.

3. DHS should make public data related to international student entry at land, sea, and air ports of entry, to include rates of admission, denial, and deferred inspection.

4. DHS should promote existing customer service programs and resources available to assist international students and school officials in understanding DHS policies and procedures.

5. DHS should allow the U.S. Immigration and Customs Enforcement (ICE) Student and Exchange Visitor Program (SEVP) to use available funding from user fees to hire staff necessary to enhance SEVIS and implement other initiatives identified in ICE SEVP's 2008 fee increase.

6. DHS should expedite plans to enhance SEVIS.

Summary of Progress

- Since March 2012, the subcommittee has proposed 24 recommendations across its three taskings, all of which have been adopted by the HSAAC.

- Please refer to the HSAAC Recommendations and DHS Aligned Accomplishments document for a detailed summary of the Subcommittee on International Students' progress to date.

Progress Report from the Homeland Security Academic Advisory Council's Subcommittee on Cybersecurity

The Subcommittee on Cybersecurity is charged with providing advice and recommendations to the Secretary and senior leadership on the following:

1. *How to attract students, student veterans and recent graduates to cybersecurity jobs at DHS*;

2. ***How can DHS better promote the DHS/National Security Agency National Centers of Academic Excellence cybersecurity programs to the higher education community*;**

3. *How to define the core elements of cybersecurity degree and certificate programs to prepare graduates for mission-critical cyber jobs at DHS*;

4. ***How DHS can facilitate and strengthen strategic partnerships with industry, national labs, colleges, universities and others to build the cybersecurity workforce*;**

5. *How DHS can partner with academia to build a pipeline of diverse students in STEM; and*

6. *How key subcategories in cybersecurity such as policy, critical infrastructure, human factors intellectual property, and others – can inform academic pathways to meet national needs.*

Chaired by San José State University President Dr. Mohammad H. Qayoumi, the subcommittee met via teleconference on September 17, 2013, January 7 and February 19, 2014, discussing taskings 2 and 4 (in bold font, above) as well as potential recommendations.

Overall Findings

- In order to address the shortage of cybersecurity professionals and build a sustainable pipeline of talent, it is important to create pathways for students to become and stay engaged in cybersecurity throughout their education (see Attachment 1: "Cybersecurity Competency Model").

- Federal government hiring qualification standards, controlled by the Office of Personnel Management, preclude applicants with Associate's degrees from qualifying for certain DHS entry-level cybersecurity positions based on education alone. Under the Pathways Program, DHS could set qualifications for intern positions and possibly qualify community college students at the GS-05 level.

- Community colleges are well-positioned to develop a large number of highly skilled cybersecurity professionals, and students who successfully complete cybersecurity programs focused on hands-on technical training will be highly sought after. DHS should explore and expand innovative partnerships with community colleges.

- DHS and the National Security Agency (NSA) partner on the strategic direction of the National Centers of Academic Excellence in Information Assurance Education (CAE/IAE), IA 2-year Education and Training (CAE/2Y), IA Research (CAE/R), and upcoming IA/Cyber Defense programs. These programs promote Information Assurance (IA) education, training, research and awareness, to produce professionals with IA expertise in various disciplines.

- Criteria for CAE designations have recently changed and will now be based on knowledge units (KUs), rather than Committee on National Security Systems (CNSS) standards. DHS produced a report recommending focus areas that map to DHS' mission critical needs in cybersecurity, which will help streamline DHS' recruitment efforts by targeting specific CAEs.

- Institutions of higher education with a CAE-designation(s) benefit by: serving as recruitment sources for the federal government; producing students with the knowledge and ability to readily join the cybersecurity workforce; sharing resources with an extended network of academic institutions; and participating in IA and capacity-building scholarship and grant opportunities (i.e. Scholarship for Service).

Draft Recommendations

The Subcommittee on Cybersecurity makes the following draft recommendations:

1. DHS should launch an internal campaign to educate program managers on the new Pathways Programs hiring authority for internships, including the options it presents for providing community college students with work experience.

2. The summer 2013 Secretary's Honors Program Cyber Student Volunteer Initiative, in which community college students served in U.S. Immigration and Customs Enforcement cyber forensics labs, should be expanded and cited as a best practice.

3. DHS should ensure that its cyber internship programs include a structured career path where participants have the opportunity to be hired for permanent entry-level positions upon completion of the program.

4. DHS should expand its internship opportunities to include virtual internships and mentorships, in order to engage additional students and strengthen the Department's cybersecurity recruitment efforts.

5. DHS and NSA should align the KUs used as criteria for CAE designations to a set of learning outcomes to help institutions of higher education developing cyber-related degree and certificate programs better meet workforce needs.

6. DHS and NSA should formally deputize CAEs to act as representatives of the program at higher education conferences and meetings to conduct outreach and promote the program's benefits to academic institutions.

Summary of Progress

- Since March 2012, the subcommittee has proposed 16 recommendations across two of its six taskings, all of which have been adopted by the HSAAC.[1]

- Please refer to the HSAAC Recommendations and DHS Aligned Accomplishments document for a detailed summary of the Subcommittee on Cybersecurity's progress to date.

[1] HSAAC recommendations from July 17, 2013 meeting are found in the transmittal memos from Chairman Loh to Secretary Johnson, located in the member briefing materials.

CYBERSECURITY DEGREE PATHWAY

COMPETENCIES + EMPLOYABILITY

CONTINUED LEARNING + PROFESSIONAL DEVELOPMENT

MD MASTER'S DEGREE

5–10 YEARS

COMPETENCY LEVELS
Expert/Senior Practitioner

CERTIFICATIONS
CISSP • Certified Information Systems Security Professional
CompTIA Advanced Security Practitioner (CASP)

CONTENT
Access Control • Telecommunications and Network Security
Information Security Governance and Risk Management
Software Development Security • Cryptography • Security Architecture and Design
Operations Security • Business Continuity and Disaster • Recovery Planning
Legal, Regulations, Investigations and Compliance
Physical (Environmental) Security • Research & Analysis
Integration of Computing, Communications,
and Business Disciplines

BD BACHELOR'S DEGREE

1–5 YEARS

COMPETENCY LEVELS
Practitioner

CERTIFICATIONS
Certified Authorization Professional (CAP)
Systems Security Certified Practitioner (SSCP)

CONTENT
Access Controls • Cryptography • Malicious Code and Activity
Monitoring and Analysis • Networks and Communications
Risk, Response and Recovery • Security Operations and Administration
Risk Management Framework (RMF) • Categorization of Information Systems
Selection of Security Controls • Security Control Implementation
Security Control Assessment • Information System Authorization
Monitoring of Security Controls

AD ASSOCIATE DEGREE

ENTRY LEVEL

COMPETENCY LEVELS
Technician

CERTIFICATIONS
CompTIA Security+
CWNA 4011
GIAC GSEC
(ISC)2 SSCP (Test)

CONTENT
Information Security Principles • Access Control • Risk Management
Information Technology Principles • Information Security Compliance
Threats, Attacks and Vulnerabilities • Security Tools and Techniques
Encryption and Cryptography • Security Operations and Activities
Audit, Testing and Monitoring Strategies • Malicious Code Activity
Information Technology Protection Mechanisms
Information Technology Ethics • Operating System
Security • Network Security

HS HIGH SCHOOL +COLLEGE

PREPARATION

COMPETENCY LEVELS
Career Readiness/Employability

CERTIFICATIONS
National Career Readiness Certificate
Employability Skills Certificate

CONTENT
Interpersonal Skills • Integrity • Professionalism • Reputation • Motivation
Dependability & Reliability • Self-Development • Flexibility & Adaptability • Ability to Learn
Mathematics • Locating, Reading & Using Information • Writing • Listening • Speaking
Engineering & Technology • Critical & Analytical Thinking • Science
Information Technology • Business Fundamentals • Teamwork • Following Directions
Planning, Organizing & Scheduling • Problem Solving & Decision Making
Ethics • Employability & Entrepreneurship
Working with Basic Tools & Technology

DEVELOPING LIFE + LEARNING SKILLS

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

DHS Campus Resilience Pilot Program

On February 1, 2013, the Department of Homeland Security (DHS) announced the launch of the DHS Campus Resilience Pilot Program (CR Pilot), an initiative that engages colleges and universities to help develop and pilot an emergency preparedness and resilience planning process. Through the program, DHS worked with seven competitively selected colleges and universities to draw on existing resources and collaborate with federal, state and local stakeholders, including the Department of Education and the Department of Justice, to identify new innovative approaches to promote campus resilience.

The CR Pilot was created upon recommendation from the Homeland Security Academic Advisory Council that DHS establish a campus resilience program. The program is a joint initiative of and is supported by DHS' Federal Emergency Management Agency (FEMA), U.S. Immigration and Customs Enforcement Student and Exchange Visitor Program, and the Office of Academic Engagement.

The CR Pilot builds upon best practices, lessons learned and resources already developed to make U.S. colleges and universities more resilient, and promotes DHS' FEMA's Whole Community approach to resilience planning. It also directly supports the goals of the President's Plan to Reduce Gun Violence by emphasizing the importance of emergency preparedness.

Facilitated engagement sessions involving campus leadership, students, and community stakeholders were held at the seven CR Pilot colleges and universities throughout the spring and summer of 2013. These sessions highlighted the needs of various student populations, particularly those of international students, and helped inform an emergency preparedness and resilience planning process.

The Campus Resilience Enhancement System

Through the CR Pilot, DHS and the Community and Regional Resilience Institute have developed the Campus Resilience Enhancement System (CaRES), a web-enabled tool that guides institutions of higher education (IHEs) through a resilience planning process in four distinct sections:

1. ***Organize:*** Users first determine the wide range of campus and community personnel involved in emergency preparedness and resilience planning at their respective IHE.
2. ***Assess:*** Through self-facilitated workshops, users measure resilience by assessing key campus service areas.
3. ***Act:*** Based on the results of these workshops, the system recommends specific actions an IHE can take to build its resilience, as well as resources, tools and crisis recovery playbook templates available to assist IHEs in their efforts.
4. ***Evaluate:*** The system provides users with sample tabletop exercises an IHE can use to test and evaluate their emergency management plans.

CaRES will help IHEs apply resilience practices to a campus environment, with tools, resources and techniques that can be embedded into their operations and planning processes. The system can be adapted to schools of all sizes and settings.

The following seven colleges and universities were selected to participate in the CR Pilot. Each engaged in extensive on-campus and virtual emergency preparedness and resilience planning.

1. **Drexel University**, Philadelphia, Pennsylvania
2. **Eastern Connecticut State University**, Willimantic, Connecticut
3. **Green River Community College**, Auburn, Washington
4. **Navajo Technical College**, Crownpoint, New Mexico
5. **Texas A&M University**, College Station, Texas
6. **Tougaloo College**, Jackson, Mississippi
7. **University of San Francisco**, San Francisco, California

Campus Resilience Enhancement System (CaRES)

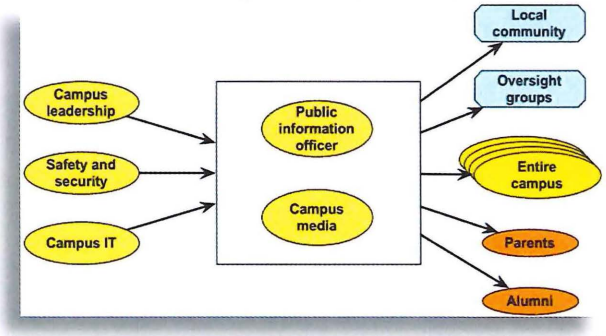
Building campus resilience in the face of disruption, turbulence and change.

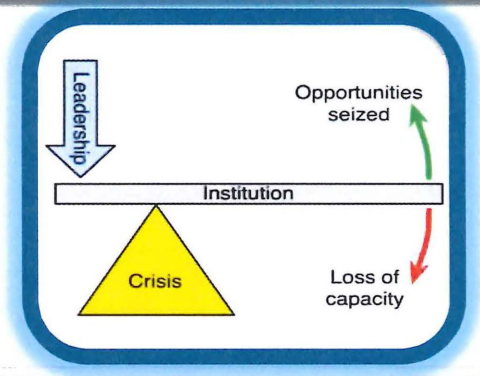
Success

A practical, usable process and tool kit developed in cooperation with our university partners.

Validated in practice and ready for implementation.

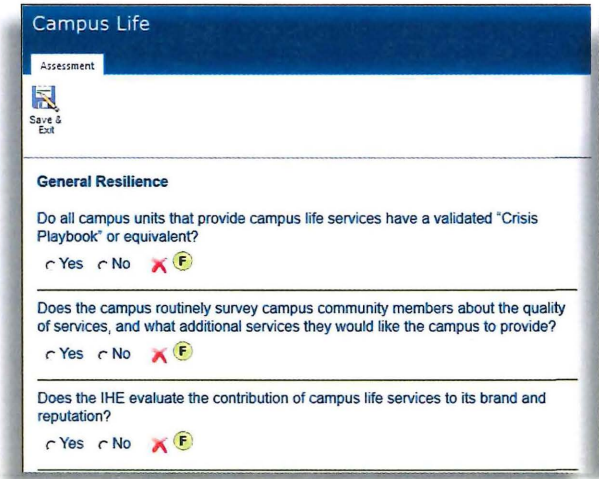
1. Organize

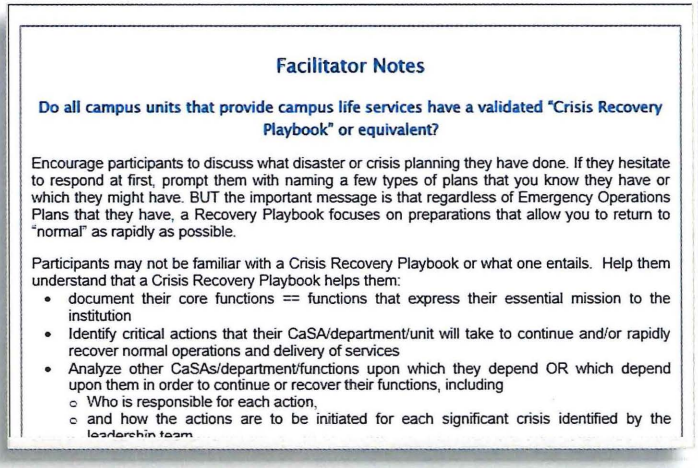




2. Assess

- Academic
- Business Services
- Campus Life
- Communications
- Cultural & Athletics
- Facilities, Campus Housing & Transportation
- Finance
- Health
- Information Technology & Records
- International Programs
- Off-Campus Housing
- Research
- Safety & Security
- Utilities





Facilitator Notes

Do all campus units that provide campus life services have a validated "Crisis Recovery Playbook" or equivalent?

Encourage participants to discuss what disaster or crisis planning they have done. If they hesitate to respond at first, prompt them with naming a few types of plans that you know they have or which they might have. BUT the important message is that regardless of Emergency Operations Plans that they have, a Recovery Playbook focuses on preparations that allow you to return to "normal" as rapidly as possible.

Participants may not be familiar with a Crisis Recovery Playbook or what one entails. Help them understand that a Crisis Recovery Playbook helps them:

- document their core functions == functions that express their essential mission to the institution
- Identify critical actions that their CaSA/department/unit will take to continue and/or rapidly recover normal operations and delivery of services
- Analyze other CaSAs/department/functions upon which they depend OR which depend upon them in order to continue or recover their functions, including
  - Who is responsible for each action,
  - and how the actions are to be initiated for each significant crisis identified by the leadership team

Meridian Institute
Connecting People to Solve Problems

CARRI Community & Regional Resilience Institute

3. Act

Cancel

Show Action Plan Items for this CaSA: International Programs

To Add New Action Plan Item: ➡Click Here

Potential Action (None) | Selected Action (Now) | Deferred Action (Later) | Declined Action (Never)

Page 1 of 1 --Select Number of Rows--

CaSA	Version	Priority	Seq	Edit	Resource
International Programs	*1399*	None	0		R

Action Verbiage:

All campus units that support international programs should develop "Crisis Recovery Playbooks" that address the unit's ability to continue operations and/or rapidly recover normal functions and delivery of services. The playbook should be validated by an exercise.

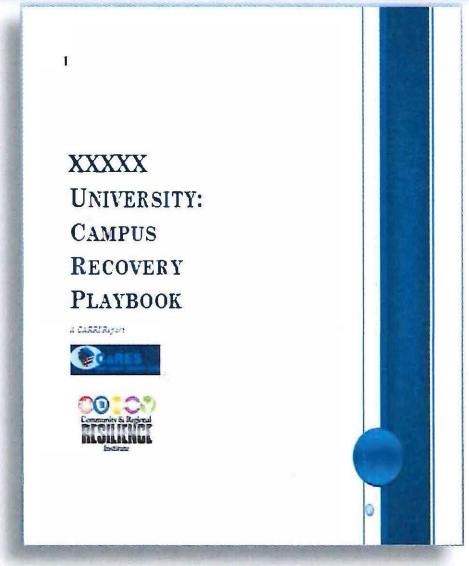
Resource

Crisis Recovery Playbooks

Below are two resources that can assist your institution in developing crisis recovery playbooks.

1. Use the CARRI Unit Level Crisis Recovery Playbook template to develop a comprehensive playbook that covers all units supporting international programs.
2. View Federal guide for developing high-quality emergency operations plans for institutions of higher education. The guide includes annexes on Family Educational Rights and Privacy Act (FERPA) and additional information that relates to international students and scholars.

CaRES Campus Resilience Enhancement System



4. Evaluate

- After-ActionReportTabletopTemplate
- ConductingSuccessfulTabletop
- ActiveShooterTabletop
- BombThreatTabletop
- FinancialCrisisTabletop
- FireandExplosionTabletop
- HazMatIncidentTabletop
- HealthIncidentTabletop
- InfoTechnologyExercise
- ScandalTabletop
- TornadoTabletop

Vision: *Create partnerships to implement CaRES nationally*

Warren Edwards
Executive Director
Community and Regional Resilience Institute (CARRI)

Warren Edwards is the Executive Director of CARRI in Oak Ridge, Tennessee. CARRI is housed at the Meridian Institute where their partnership can leverage both organizations' expertise in building collaborative foundations for resilience and stability. The mission of CARRI is to help develop and then share critical paths that any community or region may take to strengthen its ability to prepare for, respond to, and rapidly recover from significant man-made or natural disasters with minimal downtime of basic community, government, and business services. CARRI supports communities in their resilience building efforts and also works with state, regional, and national stakeholders to create incentives and support for community resilience.

After retiring as a Major General from the United States Army and before joining UT-Battelle, Edwards served as the Chief Operating Officer for Oak Ridge Technology Connections (TechConnect), LLC. In that position he established the start-up business plan, the operating systems, policies, and business procedures for a high-technology consulting enterprise and brought them to full operating capability. Prior to TechConnect, Edwards was a Senior Director for CACI, Inc. in Atlanta, Georgia. In that capacity, he established the Atlanta operations office for CACI and managed a series of programs throughout the Southeast supporting the Department of Defense and other federal agencies. During his more than 30 years of military service, Edwards held numerous positions.

Edwards graduated from the University of Richmond, Richmond Virginia and holds a Master's of Military Arts and Sciences from the US Army Command and Staff College and a Master's of Science in International Studies from the US Naval War College.

Progress Report from the Homeland Security Academic Advisory Council's Subcommittee on Campus Resilience

The Subcommittee on Campus Resilience is charged with providing advice and recommendations to the Secretary and senior leadership on the following:

1. ***How colleges and universities use specific capabilities, tools, and processes to enhance campus and community resilience as well as the cyber and physical infrastructure;***

2. *How DHS' grant programs may be adjusted to support resilience-related planning and improvements;*

3. ***How campuses can better integrate with community planning and response entities;***

4. *How to implement the whole community approach and preparedness culture within student and neighboring communities;*

5. *How to strengthen ties between DHS' Federal Law Enforcement Training Center (FLETC) and campus law enforcement professionals; and*

6. ***How DHS can better coordinate with individual campus IT departments on the risks towards and attacks on computer systems and networks.***

Chaired by University of Missouri Chancellor Dr. R. Bowen Loftin, the subcommittee met via teleconference on January 16 and February 20, discussing taskings 1, 3 and 6 (in bold font, above) as well as potential recommendations.

Overall Findings

- Through the DHS Campus Resilience Pilot Program, DHS and the Community and Regional Resilience Institute have developed the Campus Resilience Enhancement System (CaRES), a web-enabled tool that guides institutions of higher education (IHEs) through a resilience planning process.

- The Department of Justice (DOJ) National Center for Campus Public Safety (National Center) was recently established and will serve as a clearinghouse of campus public safety information and resources for IHEs. It will also convene leaders from government and the academic community to conduct research and develop guidance and best practices on issues related to campus public safety.

- The DOJ/Federal Bureau of Investigation's (FBI) National Security Higher Education Advisory Board (NSHEAB) is comprised of presidents and chancellors of several prominent U.S. universities, and is designed to foster outreach and promote understanding between higher education and the FBI. NSHEAB does consider some issues that are relevant to the HSAAC.

- The Federal Emergency Management Agency (FEMA), through its Emergency Management Institute, frequently engages with the higher education community on campus preparedness and resilience efforts. Of note, on a regional and local level, New England's FEMA Region 1 is affiliated with over 170 colleges and universities and works closely with the Region 1

International Association of Emergency Management University and College Caucus, the IHEs and other stakeholders to provide resources and tools through regular coordination and collaboration.

- While IHEs share tabletop and emergency planning exercises and best practices, it is on an ad-hoc basis. IHEs would benefit from additional methods of sharing these tools and processes.

Draft Recommendations

The Subcommittee on Campus Resilience makes the following draft recommendations:

1. DHS should continue to support its Campus Resilience Pilot Program as funding allows.

2. DHS should partner with the DOJ National Center to promote campus resilience as well as offer CaRES as a resource to the broader higher education community.

3. Through the Homeland Security Academic Advisory Council, DHS should establish a partnership with the DOJ/FBI NSHEAB to promote information sharing and collaboration on cybersecurity-related and other issues that are common to both groups.

4. FEMA's Region 1 should be recognized as a DHS best practice for engagement with the higher education community on campus preparedness and resilience efforts.

5. DHS should explore situational awareness and information sharing resources and tools such as DHS' Virtual USA and commercial solutions that enable IHEs to better share best practices and coordinate on campus resilience, preparedness and response issues.

6. DHS should create an online repository of downloadable tabletop exercises specific to colleges and universities. This should include exercises developed by other IHEs that can be adapted and modified to fit the specific needs of the user.

Summary of Progress

- Since March 2012, the subcommittee has proposed 14 recommendations across five of its six taskings, all of which have been adopted by the HSAAC.

- Please refer to the HSAAC Recommendations and DHS Aligned Accomplishments document for a detailed summary of the Subcommittee on Campus Resilience's progress to date.

Progress Report from the Homeland Security Academic Advisory Council's Subcommittee on Student and Recent Graduate Recruitment

The Subcommittee on Student and Recent Graduate Recruitment is charged with providing advice and recommendations to the Secretary and senior leadership on the following:

1. ***How to attract student interns, student veterans, and recent graduates to jobs at DHS;***

2. *How to use social media and other means of communication to most effectively reach this audience; and*

3. ***How to ensure that students and recent graduates of Historically Black Colleges and Universities, Hispanic Serving Institutions, Tribal Colleges and Universities, and other Minority Serving Institutions know of and take advantage of DHS internship and job opportunities.***

Chaired by Saint Augustine's University President Dr. Dianne Boardley Suber, the subcommittee met via teleconference on January 30, discussing taskings 1 and 3 (in bold font, above) as well as on-going DHS initiatives.

Recent Discussion(s)

- In 2014, DHS launched the second phase of the Secretary's Honors Program (SHP) Cyber Student Volunteer Initiative (CSVI). Originally created in 2013, the program expanded to new DHS offices and locations in 2014, with over 100 unpaid student volunteer assignments available in over 60 locations across the country. Through the program, selected student volunteers will gain hands-on experience and exposure to the cybersecurity work performed by DHS cybersecurity professionals. DHS conducted targeted outreach to over 330 schools nationwide to encourage students to apply, and approximately 605 eligible candidates applied for the program through the USAJobs vacancy announcement (see Attachment 1: "DHS SHP CSVI Overview").

- DHS transmitted draft Department-wide Memoranda of Understanding (MOUs) to the following Higher Education Associations (HEAs): American Association of Community Colleges; American Indian Higher Education Consortium; Asian American and Pacific Islander Association of Colleges and Universities; Hispanic Association of Colleges and Universities; and National Association for Equal Opportunity in Higher Education.

- The intent of the MOUs is to enhance communication and cooperation, and expand outreach to and recruitment of students and recent graduates for DHS opportunities, including, but not limited to, internships, fellowships, temporary federal employment, and permanent federal employment.

Next Steps

- DHS will finalize and execute the MOUs with the aforementioned HEAs.

- The subcommittee will provide input on the implementation of the MOUs between DHS and HEAs.

Summary of Progress

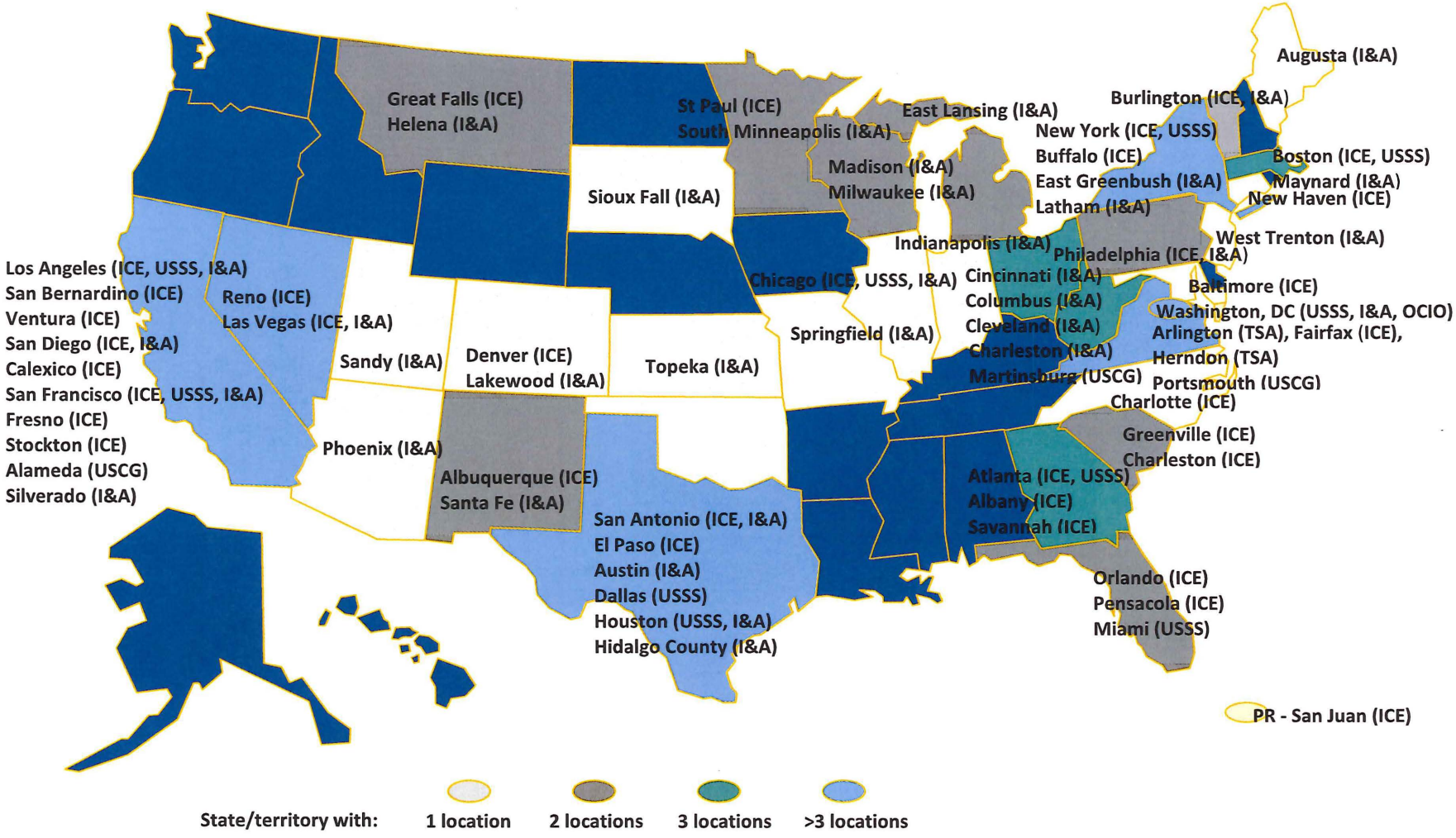
- Since March 2012, the subcommittee has proposed 14 recommendations across two of its three taskings, all of which have been adopted by the HSAAC.

- Please refer to the HSAAC Recommendations and DHS Aligned Accomplishments document for a detailed summary of the Subcommittee on Student and Recent Graduate Recruitment's progress to date.

DHS Secretary's Honors Program Cyber Student Volunteer Initiative

In April 2013, DHS announced the pilot of the Secretary's Honors Program (SHP) Cyber Student Volunteer Initiative (CSVI) through which community college student volunteers completed hands-on cybersecurity assignments at U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) field offices and state and major urban area fusion centers between June and September 2013.

In December 2013, DHS announced the launch of the 2014 SHP CSVI. In this second iteration of the program, 116 unpaid college student volunteer assignments will be available to support DHS' cyber mission at local DHS field offices in over 60 locations across the country. The program has been broadened to include opportunities at the U.S. Secret Service (USSS), the U.S. Coast Guard (USCG), the Transportation Security Administration (TSA), the Office of Intelligence and Analysis (I&A), the DHS Office of the Chief Information Officer (OCIO), and additional ICE HSI forensics labs and state and major urban area fusion centers. Student assignments, which are expected to be completed between April and September 2014, will include challenging work projects, real-life scenarios, and mentoring from cybersecurity professionals. The SHP CSVI is centrally managed by the CyberSkills Management Support Initiative team, through the Office of the Chief Human Capital Officer, in coordination with the Office of Academic Engagement, the Science and Technology Directorate, and participating DHS Components.



Progress Report from the Homeland Security Academic Advisory Council's Subcommittee on Academic Research and Faculty Exchange

The Subcommittee on Academic Research and Faculty Exchange is charged with providing advice and recommendations to the Secretary and senior leadership on the following:

1. *How academic research can address DHS' biggest challenges;*

2. *How DHS operational Components can form lasting relationships with universities to incorporate scientific findings and research and development (R&D) into DHS' operations and thought processes;*

3. *How universities can effectively communicate to us emerging scientific findings and technologies that will make DHS operations more effective and efficient;*

4. ***How we can jointly create a robust staff/faculty exchange program between academe and DHS;*** *and*

5. *How DHS assesses the risk and value of its major programs.*

Chaired by Northeastern University President Dr. Joseph E. Aoun, the subcommittee met on January 23, discussing tasking 4 (in bold font, above) as well as potential recommendations.

Overall Findings

- DHS has a vested interest in leveraging its Loaned Executive Program and Intergovernmental Personnel Act (IPA) Mobility Program to strengthen its engagement and partnership with the academic community.

- The Loaned Executive Program is a special unpaid opportunity for top executive-level experts from the private sector to share their expertise at DHS.

- The IPA Mobility Program provides a temporary assignment of personnel between the Federal government and state, local and tribal governments; colleges and universities; federally funded research and development centers; and other eligible organizations.

Draft Recommendations

The Subcommittee on Academic Research and Faculty Exchange makes the following draft recommendations:

1. DHS should leverage the IPA Mobility Program to formally establish an Academic Exchange Program that consists of the following three components: (1) Academic Speakers Bureau; (2) Guest Lecturer Series; and (3) Faculty Exchange Program.

2. The DHS Academic Exchange Program should include the following programmatic elements: (1) targeted outreach to IHEs to enhance visibility; (2) appropriate titles for program participants (i.e. Senior Fellows, Junior Fellows, etc.); and (3) when possible, a cost-sharing mechanism between DHS and participating IHEs.

3. DHS should compile a list of the specializations and/or priorities of its Components to determine the types of IHE faculty/staff and DHS personnel that should participate in the Academic Exchange Program. In support of this, DHS should use the list of 34 DHS priority research topics compiled by DHS' Science & Technology Directorate in July 2013 to identify potential program participants.

Summary of Progress

- Since March 2012, the subcommittee has proposed four recommendations across three of its five taskings, all of which have been adopted by the HSAAC.

- Please refer to the HSAAC Recommendations and DHS Aligned Accomplishments document for a detailed summary of the Subcommittee on Academic Research and Faculty Exchange's progress to date.

Progress Report from the Homeland Security Academic Advisory Council's Subcommittee on Homeland Security Academic Programs

The Subcommittee on Homeland Security Academic Programs is charged with providing advice and recommendations to the Secretary and senior leadership on the following:

1. *How to define core elements of a homeland security degree at the associate's, bachelor's and master's levels;*

2. *How to apply the TSA Associates Program model to other segments of the DHS workforce who wish to pursue a community college pathway;*

3. *How to form relationships with 4-year schools so that our employees' credits transfer towards a higher level degree;*

4. *How to enhance existing relationships between FEMA's Emergency Management Institute and the higher education community to support Presidential Policy Directive 8 (PPD-8), expand national capability, and support a whole community approach;*

5. *How to expand DHS cooperation with the Department of Defense (DOD) academies and schools to provide DHS' current employees with educational opportunities;*

6. ***How colleges and universities might offer academic credit for DHS training;*** *and*

7. *How to better promote degree and certificate programs to DHS employees who are seeking professional development.*

Co-Chaired by LaGuardia Community College President Dr. Gail O. Mellow and U.S. Coast Guard Academy Superintendent Rear Admiral Sandra Stosz, the subcommittee met via teleconference on January 9, discussing tasking 6 (in bold font, above) as well as potential recommendations.

Overall Findings

- DHS is seeking to expand opportunities to provide homeland security-focused training by partnering DHS training facilities with colleges and universities in a way that would also provide academic credit for participants.

- The Federal Law Enforcement Training Center (FLETC) partners with the College of Coastal Georgia (CCGA) to provide up to 12 hours of academic credit for college coursework in the Criminal Justice discipline at CCGA.

- FLETC currently has a limited number of partnerships with other institutions of higher education, and is pursuing additional partnerships with universities and technical colleges. A number of DHS training facilities across multiple Components could potentially offer partnering opportunities.

- The Department of Defense's (DOD) Defense Activity for Non-Traditional Education Support (DANTES) is a model that DHS could utilize to expand on FLETC's current partnerships.

Draft Recommendations

The Subcommittee on Homeland Security Academic Programs makes the following draft recommendations:

1. DHS should make available a list of DHS training facilities to promote transparency in homeland security training options.

2. DHS should consider new partnerships between DHS training facilities and academic organizations and institutions that would provide participants the ability to earn academic credit for homeland security-focused coursework. These opportunities could include on-site and/or online training offered by colleges and universities.

3. DHS should explore opportunities to leverage an academic credit-based professional education model, such as DOD's DANTES, to provide DHS employees with enhanced access to continuing education.

Summary of Progress

- Since March 2012, the subcommittee has proposed 11 recommendations across two of its seven taskings, all of which have been adopted by the HSAAC.

- Please refer to the HSAAC Recommendations and DHS Aligned Accomplishments document for a detailed summary of the Subcommittee on Homeland Security Academic Programs' progress to date.

Chris Cummiskey
Under Secretary for Management (Acting)
Department of Homeland Security

Chris Cummiskey was appointed Acting Under Secretary for Management at DHS in September, 2013. One of four Under Secretaries at DHS, Cummiskey oversees the Management Directorate's programs, processes, and people through the six line of business chiefs: the Chief Financial Officer, the Chief Information Officer, the Chief Human Capital Officer, the Chief Procurement Officer, the Chief Readiness Support Officer, and the Chief Security Officer. He also serves as the DHS Chief Acquisition Officer overseeing $19 Billion in acquisition programs ranging from cyber security to aviation security.

Cummiskey has been a member of the department's executive leadership team as Deputy Under Secretary for Management from May 2010 to September 2013 and earlier as the Chief of Staff for the Management Directorate from March 2009 until May 2010. He co-chairs the DHS Executive Steering Committee on the National Cybersecurity Protection System, which has a lead role in protecting the Federal Government's cybersecurity networks. He also serves on the DHS Executive Leadership Committee overseeing the government-wide implementation of President Obama's Cybersecurity Executive Order and Presidential Policy Directive on Protecting Critical Infrastructure. Additionally, he provides expertise and oversight on the implementation of the Homeland Security Advisory Council's Cyberskills Task Force recommendations, which provide an action plan for attracting, growing and retaining top cyber talent at the department.

Prior to joining DHS, Cummiskey was the Chief Information Officer for the State of Arizona. Appointed by Governor Janet Napolitano in 2003, he advanced the Governor's agenda of innovation and government transformation through the use of technology. In 2007, Cummiskey led the effort to create the state's first information security plan and hired Arizona's first Chief Information Security Officer. As a member of the Governor's cabinet, Cummiskey chaired several key executive initiatives during his tenure. In 2008, he received the Distinguished Service to State Government Award from the National Governor's Association for his work on innovation and government transformation.

Cummiskey was elected to the Arizona State Legislature at the age of 26 and served in the House and Senate from 1991 through 2002. During his tenure in the Senate, Cummiskey held many leadership posts including that of Floor Leader. As a Senator, he was a recognized leader in the promotion of E-government, emerging technologies and the New Economy.

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Homeland Security Academic Advisory Council
Wednesday, November 20, 2013 Teleconference
Meeting Minutes

The meeting of the Homeland Security Academic Advisory Council (HSAAC) was convened from 11:02 a.m. to 11:37 a.m. via teleconference. The meeting was non-deliberative, therefore it was not posted for public notice or accessible to the public.

The following individuals were in attendance:

HSAAC Members

Dr. Wallace D. Loh, *Chair*
Dr. R. Bowen Loftin, *Vice Chair*
Dr. Lezli Baskerville
Dr. Rufus Glasper
Dr. Jay Gogue
Ms. Marlene M. Johnson
Dr. Eric W. Kaler
Dr. Gail O. Mellow
Dr. Mohammad H. Qayoumi

Department of Homeland Security (DHS) Personnel

Mr. Chris Cummiskey, Under Secretary for Management (Acting)
Ms. Lauren Kielsmeier, Executive Director for Academic Engagement

Call to Order, Opening Remarks, Introductions and Overview of the Day

Executive Director Kielsmeier called the meeting to order at 11:02 a.m. Dr. Wallace Loh, HSAAC Chair, thanked DHS staff and HSAAC members, and gave an overview of the meeting. Chair Loh noted that the teleconference was scheduled as a result of the extended government shutdown in October that forced a number of the scheduled HSAAC subcommittee meetings to be cancelled. Chair Loh also noted that the teleconference would not be deliberative in nature, allowing the HSAAC to convene without public notice and remain compliant with the Federal Advisory Committee Act, under which the HSAAC operates. Chair Loh then introduced DHS Acting Under Secretary for Management (AUSM) Chris Cummiskey.

Remarks of the Acting Under Secretary for Management/DHS Response to HSAAC Progress

AUSM Cummiskey thanked the members of the HSAAC for their service. Since its establishment, the HSAAC has adopted and transmitted 67 recommendations for consideration by DHS; many are being implemented. AUSM Cummiskey shared DHS' recent progress in implementing some of these recommendations.

With regard to the HSAAC Subcommittee on Cybersecurity, AUSM Cummiskey noted that DHS leadership is currently in the process of reviewing the subcommittee's 16 recommendations adopted by the HSAAC at its July 17, 2013 meeting.

AUSM Cummiskey discussed DHS' efforts to better publicize and promote the work of the HSAAC and the Department's progress in implementing their recommendations. DHS recently launched several new web pages on DHS.gov dedicated to the topic of academic engagement, which also highlight the HSAAC as one of the Department's key initiatives. In the coming months, DHS will continue to increase its outreach to the higher education community to better communicate the HSAAC's recommendations and the Department's accomplishments in addressing them.

AUSM Cummiskey noted that Congress is in the process of confirming Mr. Jeh Johnson as the new Secretary of Homeland Security and DHS senior leadership will work in coordination with the new Secretary to continue to build on the HSAAC's progress. DHS plans to renew the HSAAC charter in early 2014.

HSAAC Administrative Items

Executive Director Kielsmeier discussed key HSAAC membership changes. Dr. Loh has served as HSAAC Chair since its establishment in March 2012 and will end his term as chair in March 2014. Effective March 2014, Dr. R. Bowen Loftin, Chancellor of the University of Missouri, will officially become the HSAAC Chair.

Executive Director Kielsmeier announced the resignations of Dr. Hunter Rawlings, President of the Association of American Universities and Dr. Holden Thorp, the Provost and Executive Vice Chancellor for Academic Affairs of Washington University in St. Louis.

Ms. Marlene Johnson, Executive Director and CEO of NAFSA: Association of International Educators, was appointed as the new co-chair of the Subcommittee on International Students.

In the coming months, DHS will be identifying two new members to serve as representatives for DHS' Centers of Excellence and women's colleges and universities.

In the coming weeks, OAE will reach out to HSAAC members to remind them of their current membership term's expiration date and gauge their interest in continuing to serve on the HSAAC; provide an opportunity to serve on other subcommittees; and send a survey to solicit feedback regarding the management of the HSAAC.

Executive Director Kielsmeier discussed the Department of Justice's Federal Bureau of Investigation's interest in having HSAAC members serve on a panel on January 28 at the University of Southern Mississippi's National Center for Spectator Sports Safety and Security.

Discussion and Next Steps

The next HSAAC meeting is scheduled for March 19, 2014 in Washington D.C. In preparation for it, Executive Director Kielsmeier will work to schedule HSAAC subcommittee meetings in coordination with the HSAAC Subcommittee chairs and members.

Adjournment

Chair Loh thanked ASUM Cummiskey, Executive Director Kielsmeier and her team. Executive Director Kielsmeier adjourned the meeting at 11:37 a.m.

United States Department of Homeland Security
Homeland Security Academic Advisory Council

1. **Official Designation:**

   Homeland Security Academic Advisory Council (HSAAC).

2. **Authority:**

   Under the Secretary's authority in Title 6, United States Code, section 451, this charter establishes the HSAAC as a discretionary committee. This committee is established in accordance with and operates under the provisions of the *Federal Advisory Committee Act* (FACA) (Title 5, United States Code, Appendix).

3. **Objectives and Scope of Activities:**

   The HSAAC will provide advice and recommendations to the Secretary and senior leadership on matters relating to student and recent graduate recruitment; international students; academic research; campus and community resiliency, security and preparedness; faculty exchanges; and cybersecurity.

4. **Description of Duties:**

   The duties of the HSAAC are solely advisory in nature.

5. **Officials to Whom the Committee Reports:**

   The HSAAC reports to the Secretary of Homeland Security.

6. **Agency Responsible for Providing Necessary Support:**

   The Department of Homeland Security (DHS) is responsible for providing financial and administrative support to the HSAAC. Within DHS, the Office of Academic Engagement will provide this support.

7. **Estimated Annual Operating Costs and Staff Years:**

   The estimated annual operating cost of the HSAAC is $280,000, which includes 1.4 staff years of support.

8. **Designated Federal Officer:**

   A full-time or permanent part-time employee of DHS shall be appointed by the Secretary as the HSAAC Designated Federal Officer (DFO). The DFO or the Alternate DFO shall approve or call HSAAC meetings, approve meeting agendas, attend all committee and subcommittee meetings, adjourn any meeting when the DFO determines adjournment to be in the public interest, and chair meetings in the absence of the Chair or Vice Chair as directed by the Secretary.

9. Estimated Number and Frequency of Meetings:

The HSAAC is expected to meet three times each year. Additional meetings may be held with the approval of the DFO. Members may be reimbursed for travel and per diem, and all travel for HSAAC business must be approved in advance by the DFO. HSAAC meetings are open to the public, unless a determination is made by the appropriate DHS official in accordance with DHS policy and directives, that the meeting should be closed in accordance with Title 5, United States Code, subsection (c) of section 552b.

10. Duration:

Continuing.

11. Termination:

This charter is in effect for two years from the date it is filed with Congress unless terminated sooner. The charter may be renewed at the end of this two-year period in accordance with section 14 of FACA.

12. Member Composition:

The HSAAC is composed of up to 23 members who are appointed by and serve at the pleasure of the Secretary of Homeland Security. To ensure a diverse, balanced membership on the HSAAC, the members shall represent institutions of higher education, community colleges, school systems and/or partnership groups as follows:

a. Up to 14 members representing the following academic institutions or organizations: state colleges and universities, community colleges, government universities, international education, women's colleges and universities, Historically Black Colleges and Universities, Tribal Colleges and Universities, Hispanic Serving Institutions, Minority Serving Institutions, or the DHS Centers of Excellence. These members are appointed to represent the viewpoint of their respective academic institution or organization and are not Special Government Employees as defined in Title 18, United States Code, section 202(a). To the extent possible, each of the interests listed shall be represented on the committee.

b. Other such individuals as the Secretary determines to be appropriate. The appropriate membership designation for each member in this category will be determined at the time of appointment by Department ethics officials.

c. Members serve terms of office of up to three years, with approximately one-third of members' terms of office expiring each year. A member appointed to fill an unexpired term serves the remainder of that term. In the event the HSAAC terminates, all appointments to the HSAAC terminate.

13. Officers:

The Secretary of Homeland Security appoints one of the members of the HSAAC as the Chair and one of the members as the Vice Chair. The Vice Chair will act as Chair in the absence or incapacity of the Chair or in the event of a vacancy in the office of the Chair. The term of office of the Chair and Vice Chair will be one year, and members may serve more than one term.

14. Subcommittees:

The DFO may approve the establishment of subcommittees for any purpose consistent with this charter. Subcommittees shall be composed of a number of HSAAC and non-HSAAC members to be determined by the DFO. The DFO, with the consultation of the HSAAC Chair, shall designate a Chair for each of the subcommittees from among the HSAAC's members.

Subcommittees may not work independently of the chartered committee and must present their work to the HSAAC for full deliberation and discussion. Subcommittees have no authority to make decisions on behalf of the HSAAC and may not report directly to the Federal Government or any other entity.

15. Recordkeeping:

The records of the HSAAC, formally and informally established subcommittees, or other subgroups of the HSAAC shall be handled in accordance with General Records Schedule 26, Item 2 or other approved agency records disposition schedule. These records shall be available for public inspection and copying, in accordance with the *Freedom of Information Act* (Title 5, United States Code, section 552).

16. Filing Date:

February 8, 2014
Department Approval Date

March 11, 2014
CMS Consultation Date

March 13, 2014
Date Filed with Congress