CYBERSECURITY EDUCATION AND WORKFORCE DEVELOPMENT WORKING GROUP CHARTER

Mission Statement

The Cybersecurity Education and Workforce Development Working Group's mission is to build a collaborative framework of educators, government, and industry to provide strategic recommendations on enhancing national cybersecurity education and workforce development by recommending policy, best practices, and tools for the implementation of innovative and comprehensive national career pathways.

Context

The Advanced Technology Academic Research Center (ATARC) Cybersecurity Education and Workforce Development Working Group is to leverage, build, align, and unify national cyber defense capability and capacity through enhanced higher education, training, workforce development initiatives and pilot programs. The CHEWD Working Group is in direct response to this mission and supports the Cybersecurity & Infrastructure Security Agency's (CISA) JCDC as discussed below:

> *[CISA's] Joint Cyber Defense Collaborative leads development of the Nation's cyber defense plans by working across the public and private sectors to help defend against cyber threats to U.S. critical infrastructure. Through this new collaboration, CISA will promote national resilience by coordinating actions across federal agencies; state, local, tribal and territorial (SLTT) partners; and private sector entities to identify, protect against, detect, and respond to malicious cyber activity targeting U.S. critical infrastructure*.
>
> CISA August 2021

The Cybersecurity Education and Workforce Development Working Group will provide a process and framework to directly engage and leverage CISA's JCDC capability, capacity, and expertise to amplify their mission, reach, and desired outcomes in order to build, maintain, and sustain a unified cyber defense. Our activity is in four distinct areas:

1. Cybersecurity Higher Education (and K-12 Education) Programs
2. Cybersecurity Higher Education Research Collaboration, Partnerships, and Initiatives
3. Cybersecurity Workforce Development: Models and Transitions into Careers
4. Educational Institution cybersecurity planning, policy, risk management, critical infrastructure protection, and information sharing.

The Cybersecurity Education and Workforce Development Working Group will consist of a diverse team representing key stakeholders and major partners to enable synchronized, holistic cybersecurity planning, cyber defense, and response through higher education, training, research, and workforce development best practices and policy. Build out a collaborative network of private sector, public sector, academia, and community-based organizations to work collaboratively at all levels of cybersecurity

education, training, and workforce development. To this end, specialized subgroups are part of The Cybersecurity Education and Workforce Development Working Group.

The Cybersecurity Education and Workforce Development Working Group will provide nationwide oversight and champion specialized working groups. The specialized working groups may be aligned by educational institutions, organizational function, geography, industry sectors, research areas, and specific events; and will ensure collaboration, lessons learned, programmatic information, and best business/ educational practices and policies flow across working groups to provide transparency and knowledge to a broader audience.

Scope

Achieving joint cyber defense collaboration requires bringing together communities of interest and influence to build the structure for collaboration, trust, and knowledge exchange. The structure is a continuous process of a myriad of purposeful and meaningful engagements that add value to the participants and the community at large. The ATARC Cybersecurity Education and Workforce Development Working Group will include the following activities and actions to promote collaboration, trust, information sharing, and knowledge exchange amongst key partners to enhance educational institution academics, research, and service-based opportunities and program development/implementation. In addition, we assist in promulgating best practices for risk management and protecting campus critical digital infrastructure.

- Operational Collaboration
    - Exercises
        - Tabletop
        - Experimental
    - Run Books
        - Create
        - Test
        - Publish
        - Share
    - Planning
- Information Sharing Engagements
    - Sectors (i.e. critical Infrastructure sectors)
    - Education/Training Pedagogy, Curriculum, and Best Practices
    - Cybersecurity Higher Education Research Initiatives and Consortiums
- Events
    - Cross industry threat sharing
    - Cybersecurity Higher Education & Research Symposia
    - Cybersecurity Competitions
- Higher Education and K-12 Education and Training Programs
    - Design, develop, implement academic programs (degrees, certificates, digital badges/microbadges/microcredentials
    - Model curriculum- K-12/Higher Education
    - Enhancing Cybersecurity Teaching: Instructors & Professors
    - Research Initiatives

- Linkages with cybersecurity workforce development, talent acquisition models, and hiring, selection, and retention of employees
    - Enhanced and seamless transitions from higher education/workforce training into cybersecurity entry level, mid level, and advanced career tracks
    - Value of Industry Recognized Pre-Apprenticeship and Registered-Apprenticeship Models for Cybersecurity workforce and incumbent workforce development.
    - Cybersecurity retention and succession planning
- Publications
    - Cybersecurity Guidance Production and Dissemination
    - Self Assessment Documents
    - Cybersecurity Higher Education, Research, Training, and Workforce
    - Development White Papers
- Software
    - Open Source
    - Compiled Freeware

Objective

The objective of the ATARC Cybersecurity Education and Workforce Development Working Group is to create a clear pipeline and pathway for cybersecurity education and training nationwide across all levels of education (kindergarten through doctoral degrees) aligned with work experience, and industry recognized certifications. This pipeline/pathway will be aligned, linked, and seamless in transition from one level of education to the next. The second objective is interact and engage with major partners, industry leaders, government organizations, security institutions, trade organizations, and educational institutions by developing, championing, planning, and conducting cyber focused engagements, information sharing, and cross organization/sector collaboration on cybersecurity higher education and workforce development initiatives and pilot programs. Organizational collaboration is intended to leverage, build, and unify the cyber defense capability and capacity of the participants and partner organizations through enhanced and synergized education and training programs of study. This facilitation will allow partners and stakeholders to learn, experience, witness, and share unified cyber defense best business and education/training practices and policies.

Deliverables

The deliverables will be:

- Annual report to Congress
- Presentation of report and recommendations
- Cybersecurity Education and Workforce Development capability-gap analysis and asset inventory- creation of a national benchmark
- Cybersecurity education and training career pipeline/pathway pilot project
- Cybersecurity model curriculum and academic standards development and promulgation
- Assist educational institutions to promote campus and student cybersecurity workforce.
- A framework for operational collaboration and exercises
- Actionable after-action reports (AAR)
- Partnerships and Engagements with National, Regional, Industry, and Sector organizations

  - NASCIO (National Association of State CIOs)
  - FBI's InfraGard
  - National Council of Information Sharing and Analysis Centers
  - Sector-based Information Sharing and Analysis Centers (ISAC)
- Partnerships and Engagements with Federal, State, and Local Governments
- Partnerships and Engagements with Higher Education and K-12 Education
- Partnerships and Engagements with Community Based Organizations
- Partnerships with Workforce Development Agencies and Organizations
- Review and recommend cybersecurity education model curriculum; workforce development training guidelines and standards
- Review and publish Best Business Practices and review of previous definitions, concepts previously completed and determine if still viable, useful or needs adjustment
- Reference matrix of provider demos aligned with functional areas that can be used for self-assessments in exercise planning, execution, and AARs

Working Group Membership

Working Group Chairs

Dr. Keith Clement, California State University, Fresno, Academic Chair
Gregory Cooper, New Mexico State University, Academic Vice Co-Chair
Eric Wall, University of Arkansas System, Academic Vice Co-Chair
Chris Rowlands, Zimperium, Industry Chair

Working Group Chairs will:

- Attend and contribute to each Working Group meeting
- Prepare the meeting agenda, solicit topics for discussion, assign members to address discussion topics, and distribute meeting materials
- Share information of relevance; provide an update/introduction at the beginning of each meeting to encourage member engagement
- Define Working Group initiatives and activities
- Assist in forming and providing feedback on deliverables

Working Group Members

Working Group Members will:

- Participate in meetings, including exchanging technical information, experiences, and best practices to develop a shared understanding of the topic(s)
- Gather information and work on group deliverables outside of meetings as needed
- Provide feedback on draft deliverables as requested
- Co-lead or participate in Sub-Working Groups (breakout teams/project teams) as needed
- Provide input on meeting agendas as requested

ATARC Support

Elizabeth Wyckoff, Associate Director, Working Groups
Amy Karpowicz, Working Group Associate
Tim Harvey, Director of Government Engagement

ATARC support will:

- Serve as program manager for the Working Group
- Coordinate and drive group projects and deliverables forward
- Schedule Working Group meetings
- Develop Working Group meeting agendas along with the chairs
- Facilitate Working Group meetings along with the chairs
- Assist in distributing relevant documents and materials to Working Group members
- Send meeting minutes, post-meeting decisions, and action items to Working Group members after each meeting
- Assist in preparing final proposals/recommendations
- Provide marketing services for the Working Group (promoting completed deliverables, etc.)
- Develop strategies to improve Working Group engagement, including applicable cross-overs with other Working Groups and relevant events
- Coordinate Working Group Labs as applicable

Rules of Engagement

The Working Group rules of engagement are described as below:

- Meet monthly from 2022 to 2024, or until amended by ATARC Support
- Follow the Working Group's ground rules developed in the charter
- Join Working Group meetings prepared and with requested action items completed
- Provide respectful and constructive feedback to yield the best decisions for the Working Group's objectives
- Final decisions are made by the Working Group Co-Chairs and ATARC Support

The Working Group will:

- Meet the first Friday of each month from 2:00-3:00 PM EST.
- Form Sub-Working Groups (breakout teams/project teams) as needed
- Follow the group's ground rules developed at one of the Working Group meetings
- Strive to make decisions by unanimous agreement. All members of the Working Group have a voice and will be listened to.
- If a Working Group member misses a meeting, decisions will be made in their absence. The Working Group will decide on a case by case basis if a decision made in the absence of a member shall be revisited.

File Sharing and Collaboration Tools

Access to the ATARC Box Account is managed by ATARC Support.

Disclaimer: Products and communications by ATARC's Cybersecurity Education and Workforce Development Working Group do not necessarily represent the plans or preferences of any company or government agency.