ATARC

19309 Winmeade Dr. Suite
446
Leesburg, VA 20176

ATARC Cybersecurity Higher Education and Workforce Development Working Group (Draft version 3.0)

September 12, 2022

Cybersecurity Higher Education and Workforce Development Working Group Mission Statement

Build a collaborative framework of key stakeholders to provide strategic recommendations on enhancing national cybersecurity education and workforce development policy and practice to implement an innovative and comprehensive national career pipeline/pathway at all levels of education/training; accessible to all, and clearly communicated through detailed "road maps" for career preparedness and college readiness tracks.

Context

The Advanced Technology Academic Research Center (ATARC) Cybersecurity Higher Education and Workforce Development (ACHEWD) 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 ACHEWD 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 ACHEWD 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 ACHEWD 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 ACHEWD Working Group.

The ACHEWD 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. ACHEWD 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.

The purpose of this document is to outline the intent, scope, objectives, and general operating model of the ACHEWD Working Group.

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 Higher 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
        - Experiential
    - 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 Higher 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 Higher 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.

Cadence and Membership
The cadence of the meeting will be the first Friday of the month from 2:00 pm E.T. to 3:00 pm E.T. The chair Keith Clement (Academic Chair), and Co-Chairs Gregory Cooper (New Mexico State University) and Eric Wall (University of Arkansas System) will facilitate an environment to present new ideas and discussion topics. This environment will allow for questions to be asked and to find resolution for current critical cybersecurity capability and skill gaps and significant national hiring concerns. A representative from ATARC will keep track of minutes/notes per meeting and make them available utilizing file sharing tools.

Every other Friday, specialized working groups will brief members of the ATARC Cybersecurity Higher Education and Workforce Development Working Group. The Specialized working updates will focus on synchronizing and collaboration beyond their charter. Each specialized working group may have a separate cadence.

Key Members

Name	Email	Agency/Business	Responsibilities
Keith Clement	kclement@mail.fresnostate.edu	Fresno State University	Academic Chair
Gregory Cooper	gcooper@psl.nmsu.edu	New Mexico State University	Co-Chair, Advisor
Eric Wall	ewall@uasys.edu	University of Arkansas System	Co-Chair, Advisor
Nicole Mandes	nmandes@atarc.org	ATARC	Manager

Specializations
Every other Friday from 2:00 pm E.T. to 3:00 pm E.T, specialized sub committees will brief members of the ATARC Cybersecurity Higher Education and Workforce Development Working Group. Specialized working group updates will focus on synchronizing and collaboration beyond their charter. Each specialized committee may have a separate cadence.

Specialized sub committees will be stood up and down based on specific objectives in support of ATARC-Cybersecurity Higher Education and Workforce Development Working Group objectives.

Rules of Engagement
The working group rules of engagement are described as below:

- Meet monthly from 2022 to 2024
- Follow the group's ground rules developed in the charter
- Decisions are made by the co-chairs

File Sharing and Collaboration Tools
Access to the ATARC Huddle Instance is managed by Nicole Mandes (nmandes@atarc.org).

Documentation Repository
Advanced Technology Academic Research Center (ATARC) Cybersecurity Higher Education and Workforce Development Working Group Folder:

Version Control

Version	Date	Author	Description
1.0	8/09/2022	JC Vega	Initial Draft for Consideration and Comment
1.1	8/22/2022	Nicole Mandes	Minor edits before finalizing
2.0	9/11/2022	Keith Clement	Significant updates.

3.0	9/12/2022	Keith Clement	Transition to WG verbiage.