

# Mountain West Cybersecurity Consortium

## 2019 Fall Conference, Minutes

Rick White, Ph.D., MWCC Chair

[rwhite2@uccs.edu](mailto:rwhite2@uccs.edu), (719)360-3805

October 21, 2019

**Chair:** Rick White, Ph.D., UCCS Interim Director for Cybersecurity Programs, [rwhite2@uccs.edu](mailto:rwhite2@uccs.edu)

**Vice-Chair:** Joe Murdock, CISSP, University of Colorado Denver, [joseph.murdock@ucdenver.edu](mailto:joseph.murdock@ucdenver.edu)

**Appendices:** Appendix A – Conference Agenda

**Introduction:** The Mountain West Cybersecurity Consortium (MWCC) held its Fall Conference on October 18<sup>th</sup> at CU Denver South, 10035 S. Peoria St., Parker, CO, 80134. The event was sponsored by the University of Colorado, Colorado Springs, with funds received under Senate Bill 18-086.

**Program:** Based on the one-day format recommended at the Spring Conference, the Fall Conference agenda was arranged as listed in Appendix A to address business in the morning, and share school experiences in the afternoon.

*Business 1: Proposed Charter.* Following the Spring Conference, the MWCC Chair drafted a proposed set of By-Laws and posted them for review and comment on the MWCC website. The first order of business was to review and comment on the proposed charter. Moderate discussion ensued, focusing on the issues described below. The proposed By-Laws will be updated and ratified at the next MWCC Spring Conference in March 2020.

- A key point of concern was membership. Participants wanted to expand membership to include not just post-secondary academic institutions, but also include “academically-affiliated organizations” to foster government and industry participation.
- By the same token, there was much discussion about whether or not to enumerate the States within the “Mountain West” region. Again, the concern was about seeming exclusive. At the conclusion of arguments, it was agreed to keep the enumeration.
- The charter proposed an MWCC organization comprised of a Chair, Vice-Chair, Members, and Subcommittees. A proposal was made to add a Board of Directors, again to foster greater participation by government and industry. A subcommittee was formed to further explore the proposal and report its recommendations.
- Participants approved a recommendation to make the Chair and Vice-Chair positions two-year, overlapping terms.
- A final recommendation was adopted to add provisions for an annual report.

*Business 2: Community Project.* In accordance with the wishes of the previous conference, the MWCC Chair developed a proposal seeking funding to support five cybersecurity summer camps next summer under the National Science Foundation (NSF) GenCyber program. If awarded, the camps will be hosted by participating MWCC institutions. Each 4-day camp would accommodate 20 students, sixth to ninth grade. MWCC hosts would assist with securing camp locations, recruiting students from rural and economically disadvantaged school districts, and providing administrative support. UCCS will field the training team to travel and present at each of the five camps according to the schedule below.

- *Camp 1: June 15 – 18*
- *Camp 2: June 29 – July 3*
- *Camp 3: July 6 – 9*
- *Camp 4: July 20 – 23*
- *Camp 5: August 3 – 6*

*Business 3: Student Competition Proposal.* During a planning teleconference in preparation for the MWCC Fall Conference, a suggestion was made to assist schools with preparing for the National Collegiate Cyber Defense Competition (NCCDC). Billed as the largest inter-collegiate cyber competition in the nation, NCCDC 2020 is scheduled to hold regional competitions across the country next March, followed by the final competition sponsored by the University of Texas San Antonio (UTSA) next June. It was suggested the MWCC could assist by scheduling competitions between participating teams within the MWCC region. Because of looming regionals in March, this suggestion was tabled for consideration for the 2021 NCCDC competition. However, participants did agree to another alternative, to invite a third-party agency to host a cyber range for competing MWCC participants. A request had already been submitted to a company in Colorado Springs, but no reply received. In the meantime, participants volunteered to approach two other companies to see if they might consider hosting a cyber range in advance of the competition. Action will need to be swift in order to meet the pending timeline.

*Business 4: Journal Opportunities.* Dr. Gary Klein reported on his efforts to expand cybersecurity programs within the UCCS College of Business. Using funds provided under SB18-086, the State Cybersecurity Initiative, he was successful in adding cybersecurity topics to all major business programs including finance and accounting. His efforts have culminated in an opportunity to launch an open journal with Sage Publishing dedicated to cybersecurity for business. The MWCC was invited to participate in this opportunity as a means for advancing research and publication in cybersecurity.

*School Updates.* After lunch, discussion was opened to participants regarding 1) teacher recruitment, 2) online experience, 3) cybersecurity general education, 4) apprenticeship programs, and 5) CAE status.

- *Teacher Recruitment.* The current shortage of cybersecurity professionals has made it especially challenging to find qualified teaching staff, primarily because of the disparity in salaries between academia and industry. All participants reported similar difficulties, but the problem was reported particularly acute among two-year colleges whose salaries are even smaller. Nobody reported a specific solution, except to maybe hire more part-time adjuncts. As discussed, though, this strategy has limited application for institutions whose accrediting agencies limit the ratio of adjuncts to tenure professors.

- *Online Experience.* As UCCS considers developing its own online cybersecurity programs, participants were asked about their experience with cheating. Anecdotal evidence suggests that cheating is more prevalent online than in the classroom. Although various strategies were discussed for reducing cheating, none can completely eliminate it. In this respect, the same can be said about classroom programs: cheating cannot be completely eliminated.
- *Cybersecurity General Education.* As phishing remains the most prevalent form of cyber-attack, participants were asked about efforts to build cybersecurity courses into general education requirements. None of the participants reported any such programs in their own schools. The discussion strayed into how to make both faculty and students better aware about phishing attacks. It was generally agreed that courses were less effective than active security measures. Specifically, conducting self-initiated random phishing attacks on faculty and students with some form of consequence was deemed the most effective approach to improving awareness.
- *Apprenticeship Programs.* Arapahoe Community College reported they were actively working to build cybersecurity apprenticeships with industry. Pikes Peak Community College reported they are doing the same. Dr. Gurvirender Tejay reported on his proposal to fund apprenticeships through the Department of Labor. If awarded, Dr. Tejay invited the MWCC to participate in the program together with UCCS. Even if it's not awarded, Dr. Tejay expressed interest in developing a smaller program together with MWCC members in Colorado.
- *CAE Status.* Participating representatives from the National Security Agency (NSA) inquired on the status of schools applying for cybersecurity Center of Academic Excellence (CAE) certification. All participants reported they had NSA CAE certification. Certification must be renewed every five years. NSA is currently revising the certification process to make it more streamlined.

**Discussion:** Despite the shorter format, the one-day conference was generally satisfactory for all that it accomplished. Perhaps most significantly, the seeds were planted for the MWCC's first collaborative projects. Still, the conference was not as well attended as in the past: of the 26 registered participants, only 15 showed. There was a failure to more strenuously market, which will be corrected before the next conference. Two participants commented that perhaps the MWCC should pool its talent to tackle bigger cybersecurity problems. After explaining this was the approach taken at the last conference, it was determined that the MWCC was not yet ready to tackle the bigger problems. It was generally agreed the MWCC needs to follow a "crawl, walk, run" strategy whereby we gain experience with some small collaborative projects before we attempt the bigger ones.

**Conclusion.** The MWCC Fall Conference succeeded in laying the groundwork for becoming a true regional collaborative organization. First, it succeeded in drafting a charter that will help it become an independent organization. Second, it got buy-in from participants in conducting its first collaborative projects. As part of this buy-in, the next conference will be conducted March 6 at Regis University in conjunction with their planning for the National Collegiate Cyber Defense Competition.

[This Page Intentionally Blank]

## **Appendix A**

### **Conference Agenda**

CU Denver South, 10035 S. Peoria St., Parker, CO 80134

- 08:00 Reception/Breakfast
- 09:00 Welcome & Introductions
- 09:15 Business 1: Proposed Charter
- 09:45 Business 2: Community Project Update
- 10:15 Business 3: Student Competition Proposal
- 11:00 Business 4: Journal Opportunities
- 12:00 Lunch
- 13:00 School Updates
  - Program Updates
  - CAE Status/Efforts
  - Online Experience
  - Staffing Experience
- 16:00 Social
- 18:00 Adjourn

[This Page Intentionally Blank]