LEARNING & PERFORMANCE RESEARCH CENTER, WASHINGTON STATE UNIVERSITY - PULLMAN

VICEROY Northwest Institute for Cybersecurity Education and Research (CySER), 2025 Evaluation Report

Dr. Olusola Adesope
Dr. Femi Johnson
Blessing Akinrotimi

June 2025

Table of Contents

VICEROY Northwest Institute for Cybersecurity Education & Research (CySER), 2025 Evaluation Report

Background

The Department of Defense (DoD) funded the establishment of the VICEROY Northwest Institute for Cybersecurity Education & Research (CySER) to prepare a highly skilled cybersecurity workforce, including ROTC cadets and DoD-aligned civilian professionals. The program integrates cybersecurity education and research with the development of essential professional competencies such as teamwork, leadership, and lifelong learning. Washington State University leads this initiative and collaborates with three other universities, including the University of Idaho, Montana State University, and Central Washington University.

August 2024 – May 2025 Outcome Achievements

This evaluation report, prepared by the external evaluator, Dr. Olusola Adesope, draws on data gathered from evaluation meetings with project investigators, Qualtrics survey responses from participants, and program documentation. The purpose of this report is to assess the extent to which CySER met its annual objectives and to evaluate the program's readiness for continued success in the subsequent year.

Key achievements this funding year:

- A total of 11 seminars were delivered across two academic semesters—five in Fall 2024 and six in Spring 2025. The seminars were actively promoted by the PI team and achieved strong engagement, with an average attendance of 33 participants per session.
- Successful recruitment of students from diverse academic disciplines, including Cybersecurity, Computer Science, Management Information Systems, and Social Sciences.
- A one-week summer workshop, hosted on the Pullman campus, was successfully administered. The event featured robust participation and included two educational field trips. Further details are provided in a subsequent section.
- Twenty-one undergraduate students were selected for the 2025 VICEROY MAVEN and ENVOY internships.
- Fifty-eight students earned cybersecurity industry certifications, enhancing their workforce readiness.

- Twenty undergraduate students were engaged in cybersecurity projects at varying levels of involvement.
- The 2025 summer workshop included twelve student poster presentations, showcasing undergraduate research.
- Graduate research assistants actively served as mentors to undergraduate participants, contributing to a supportive research training environment.
- Five WSU students presented research posters at the VICEROY (virtual) symposium, expanding the visibility of CySER student research.
- Twenty-one students from the WSU Cybersecurity Club participated in the National Cyber League Fall 2024 competition, demonstrating applied learning and competitive engagement.
- A group of CySER faculty published a peer-reviewed article in IEEE Security and Privacy, focusing on the outcomes and structure of CySER summer workshops.
- The program continues to support a diverse student population, with notable representation from American, Asian, Hispanic, African American, and Female students.

Overall Assessment: CySER has demonstrated strong progress toward its objectives this reporting period, with measurable successes across student engagement, research participation, professional development, and diversity. The program is well-positioned to sustain and build upon these achievements in the upcoming year.

Fall 2024 Seminar

The Fall 2024 seminar series consisted of five expert-led presentations that explored emerging topics in cybersecurity research, education, and career development. The seminars covered a diverse range of issues, including software verification, AI and privacy in space technology, critical infrastructure security, identity fraud prevention, and trust in digital environments. The topics were as follows:

- Correctness and Verification Using Software Contracts
- Does Space AI Security Matter? Unlocking Privacy-Preserving Federated LEO Satellite Learning for Border Threat Detection
- Building Trust in an Untrustworthy World
- Securing our Critical Infrastructure – Who is CISA and how can we help?
- The Importance of Creating a Physical and Digital Identity Strategy to Combat Fraud

Methods

Participants' Demographics

The Fall 2024 seminar series featured five presentations and was held on the following dates: October 1, October 8, October 22, November 5, and November 19. Attendance at the seminar

ranged from a minimum of 30 to a maximum of 50 participants. Attendees included undergraduate and graduate students, as well as faculty members, indicating strong institutional engagement. To assess participant experiences, a post-seminar survey was administered at the end of each session. On average, across the five seminars, twenty-three participants completed the survey. The demographic breakdown of respondents was as follows:

- Gender**:** 63% Male, 36% Female, and 1% prefer not to disclose.
- Ethnicity**:** 75% White/Caucasian, 14% Asian, 8% Hispanic, 2% Other, and 1% Black/African American.

(Refer to Figures 1 and 2 for detailed demographic visualizations).

The survey instrument included 15 items, comprising a combination of open-ended, closed-ended, and demographic questions (see Appendix A). This report synthesizes participant feedback and evaluates changes in participants' knowledge and perceptions regarding cybersecurity concepts resulting from seminar engagement.

Figure 1. Fall 2024 Participants' Gender

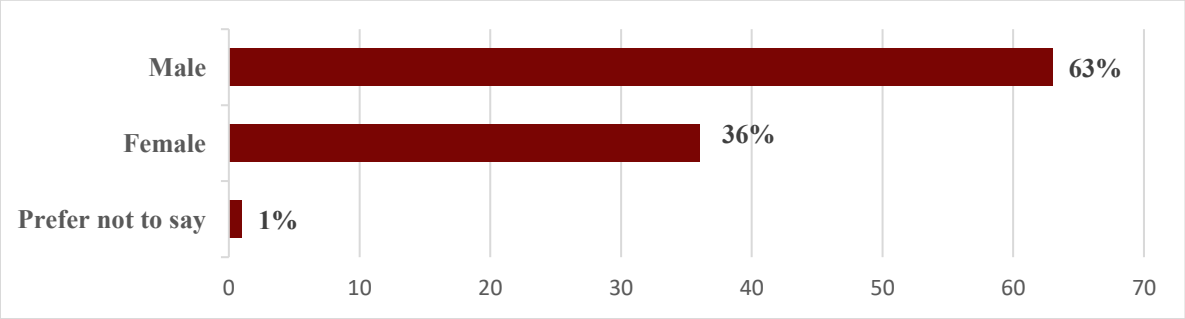
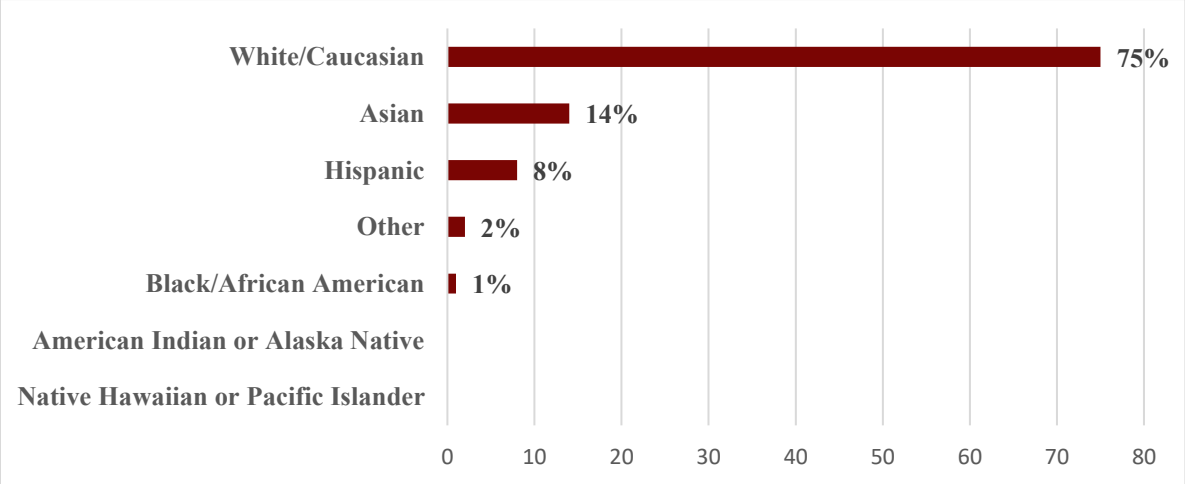


Figure 2. Fall 2024 Participants' Ethnicity



Key Findings:

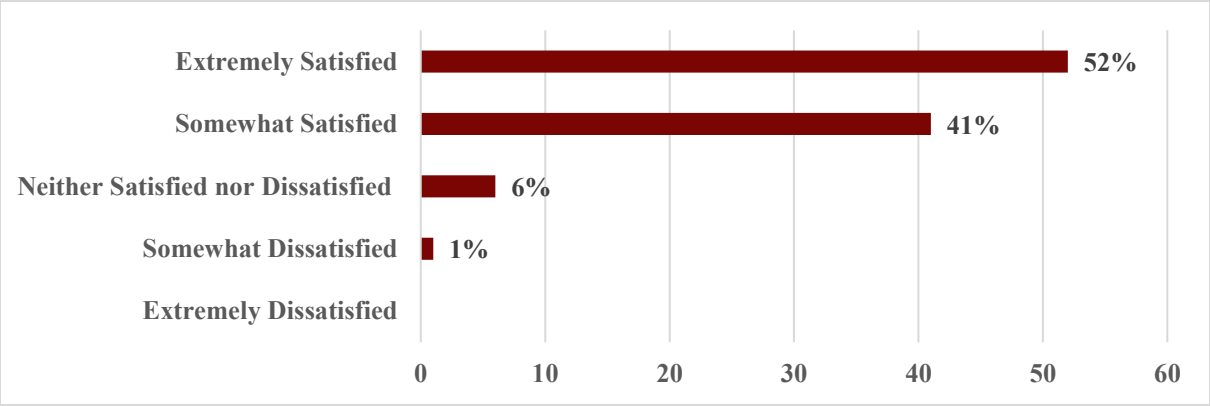
Participants' Perceived Satisfaction:

Participants rated their overall satisfaction with the Fall 2024 seminar series on a scale from *extremely dissatisfied* to *extremely satisfied*. The results indicate a high level of satisfaction across the five seminars:

- 52% rated being *extremely satisfied*
- 41% reported *somewhat satisfied*
- 6% indicated their satisfaction as *neutral (neither satisfied nor dissatisfied)*
- 1% rated being *somewhat dissatisfied*

The findings indicate a consistently high level of satisfaction among participants
(See Figure 3. Participants' Perceived Satisfaction for the Fall 2024 Seminar Series).

Figure 3. Participants' Perceived Satisfaction for the Fall 2024 Seminar Series



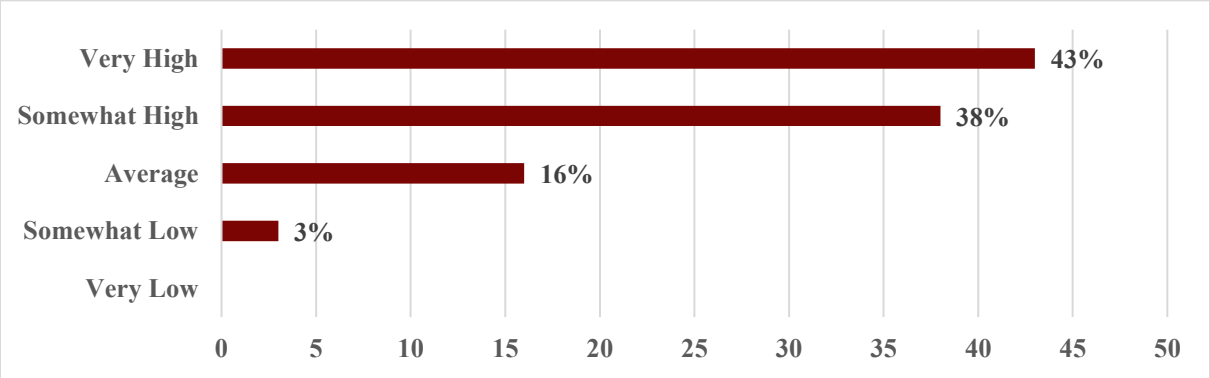
Seminars' Effectiveness in Promoting Learning:

Participants also assessed the effectiveness of the seminars in promoting their understanding of cybersecurity concepts. The results indicate a high degree of perceived instructional effectiveness:

- 43% rated the seminars as having *very high effectiveness*
- 38% reported *somewhat high effectiveness*
- 16% rated the effectiveness as *average*
- 3% indicated *somewhat low effectiveness*

This suggests that the majority of participants found the seminars to be valuable in supporting their cybersecurity learning goals.
(See Figure 4. Participants' Perceived Effectiveness for the Fall 2024 Seminar Series).

Figure 4. Participants' Perceived Effectiveness for the Fall 2024 Seminar Series



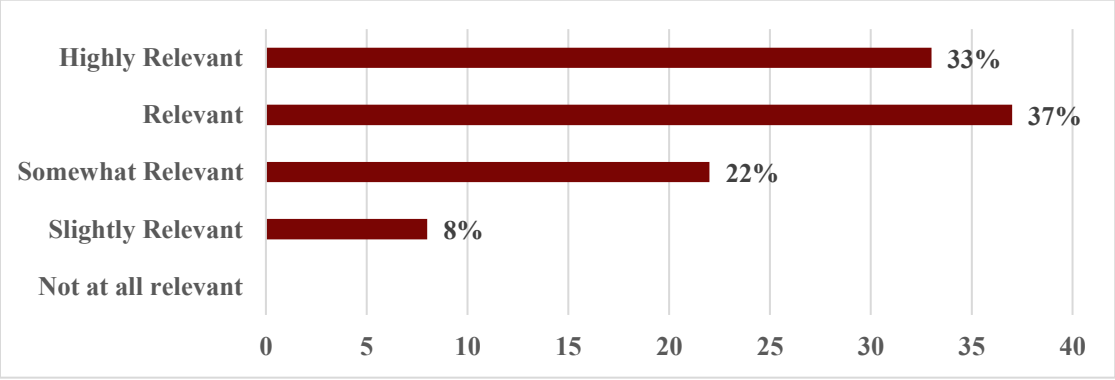
Seminars' Relevance to Participants' Need or Interest

The survey also evaluated the relevance of the seminar topics and activities to the participants' needs and interests. Participants rated the content's relevance on a scale ranging from *not at all relevant* to *highly relevant.* The results indicated that the seminars were generally well-aligned with participants' interests

- 33% rated the seminar as *highly relevant*
- 37% indicated the seminar to be *relevant*
- 22% reported the seminar to be *somewhat relevant*
- 8% rated the seminar as *slightly relevant*

The alignment between content and audience relevance underscores the seminars' potential to inform both academic and professional development.
(See Figure 5. Participants' Perceived Relevance for the Fall 2024 Seminar Series).

Figure 5. Participants' Perceived Relevance for the Fall 2024 Seminar Series



Positive Feedback:

Participants' responses reflected a high level of satisfaction with both the content and delivery of the Fall 2024 seminar series. Many attendees emphasized that the sessions were highly relevant

and educationally valuable, particularly in enhancing their understanding of core cybersecurity concepts. Many appreciated the clarity and intuitiveness of the presentation slides, especially when complemented by real-world examples, visual aids, and relatable analogies. The integration of demonstrations, practical models, and simplified explanations rendered complex technical material more accessible to a diverse audience. Additionally, the participants valued the exploration of career pathways and roles within government agencies, in broadening their awareness of opportunities in the cybersecurity field. Lastly, the engaging presentation styles, clear communication, and responsiveness to questions enabled both novice and advanced learners to benefit from the sessions.

Direct Quotes from Participants:

- *"I found the visuals in the seminar very helpful for understanding the topic."*
- *"The slides were relatively intuitive with examples that grabbed my attention."*
- *"I liked that it was more grounded in the real world and not too theoretical."*
- *"The speaker was very knowledgeable and good at answering questions if they came up."*
- *"Background information being explained and information on opportunities and internships being shared were particularly helpful."*

These comments underscore the positive reception of the seminar format and content, affirming the instructional quality and relevance of the series.

Need for Improvements:

While overall feedback on the Fall 2024 seminar series was positive, participants also identified several areas for improvement, particularly concerning content accessibility and delivery effectiveness. A recurring theme in the feedback concerned technological and communication barriers. Several participants reported difficulty understanding the speaker due to low virtual audio quality or pronunciation challenges, which hindered comprehension of key concepts. In addition, some sessions moved quickly through dense technical material, making it difficult for those with low prior knowledge in cybersecurity to follow the discussion. Participants recommended the inclusion of real-world case studies, practical demonstrations, and more visual aids to support learning and bridge the gap between theoretical content and applied understanding. These enhancements, particularly when paired with clearer pacing and more engaging delivery, were seen as critical to improving accessibility and learning outcomes for all audience members.

Direct Quotes from Participants:

- *"I found it challenging to connect it with present day examples. I would've liked a physical example or case study, so I can see it in action. Or maybe a way to put the learning into practice."*

- *"I would like to advise speakers to really bring in examples, like visuals, for students to understand the topic. I think it's especially important for students like myself who do not hold previous knowledge."*
- *"The speaker kept cutting out for me."*
- *"Mic quality, it took a lot of focus to understand what was being said."*

These suggestions offer actionable guidance for future iterations of the seminar series, particularly as the program continues to engage a diverse audience with varying levels of cybersecurity expertise.

Spring 2025 Seminar

The Spring 2025 seminar series comprised six expert-led presentations focused on cybersecurity research, education, and career development. The sessions addressed a range of timely and critical topics, including cyber-physical system security, organizational defenses, smart grid vulnerabilities, and infrastructure protection. The seminar topics were:

- Are Machine Learning Detectors Sufficient? Exploring Cyberattacks and Defense Strategies in Smart Grids
- CyberCorps Scholarship for Service Program at WSU: Developing the Next-Generation Cyber Workforce
- Emerging Technologies for Cyber-Physical Power System Security
- Practical Cybersecurity Defenses for Organizations of Any Size
- Operational Technology Cybersecurity in the Chemical Process Industries: Implications of Compromised Distributed Control Systems and Safety Instrumented Systems
- Securing Washington State Energy Critical Infrastructure

Method

Participants' Demographics

The six seminar sessions were held on the following dates: February 11, February 25, March 4, March 18, April 1, and April 15. Each session drew between 20 and 32 attendees. Attendees included undergraduate and graduate students, as well as principal investigators from consortium institutions. Following each seminar, participants completed a survey designed to assess learning outcomes and overall experience. The survey comprised 15 items, including open-ended, closed-ended, and demographic questions (refer to Appendix A for the seminar survey). Demographic data from survey respondents indicated the following:

- Gender: 62% Male, 37% Female, 1% Prefer not to disclose.
- Ethnicity: 73% White/Caucasian, 13% Asian, 7% Black/African American, 6% Hispanic, 1% Other.

(Refer to Figures 6 and 7 for graphical representations of participants' gender and ethnicity).

Figure 6. Spring 2025 Participants' Gender

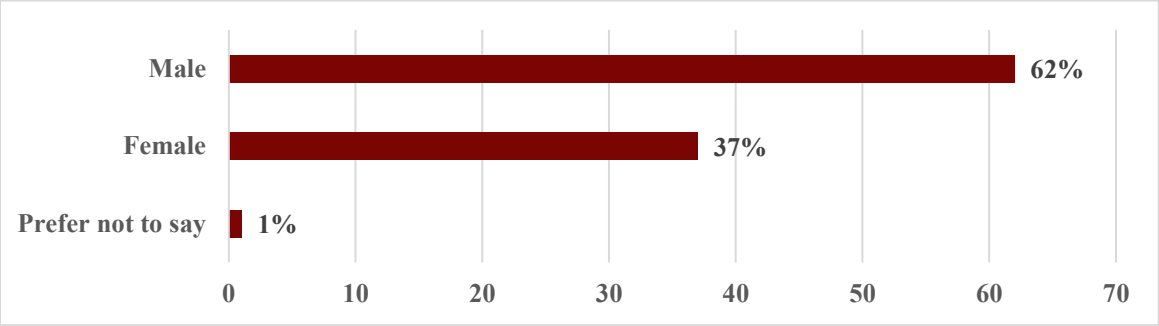
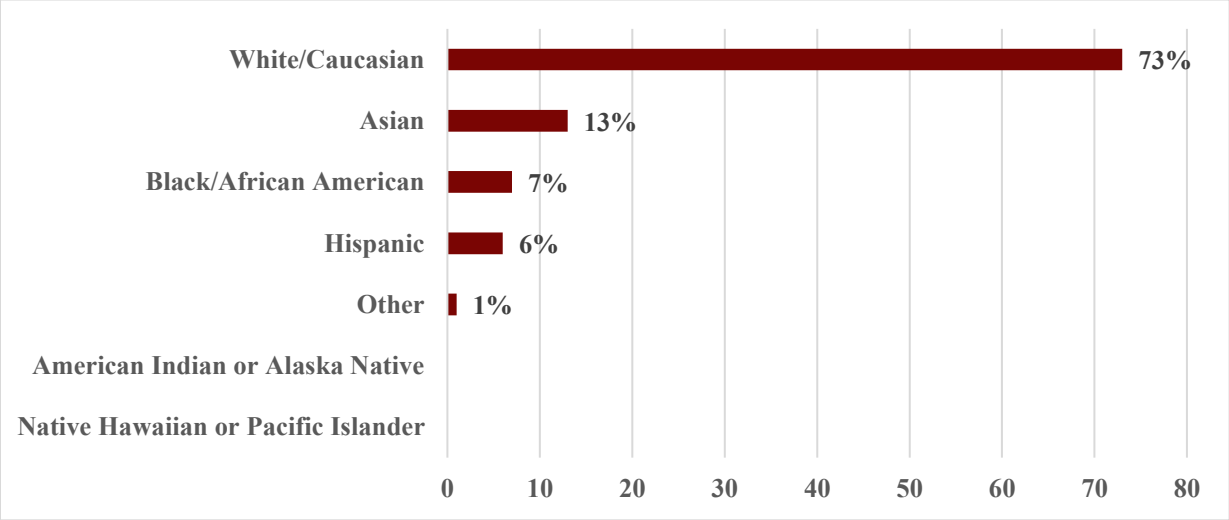


Figure 7. Spring 2025 Participants' Ethnicity



Key Findings

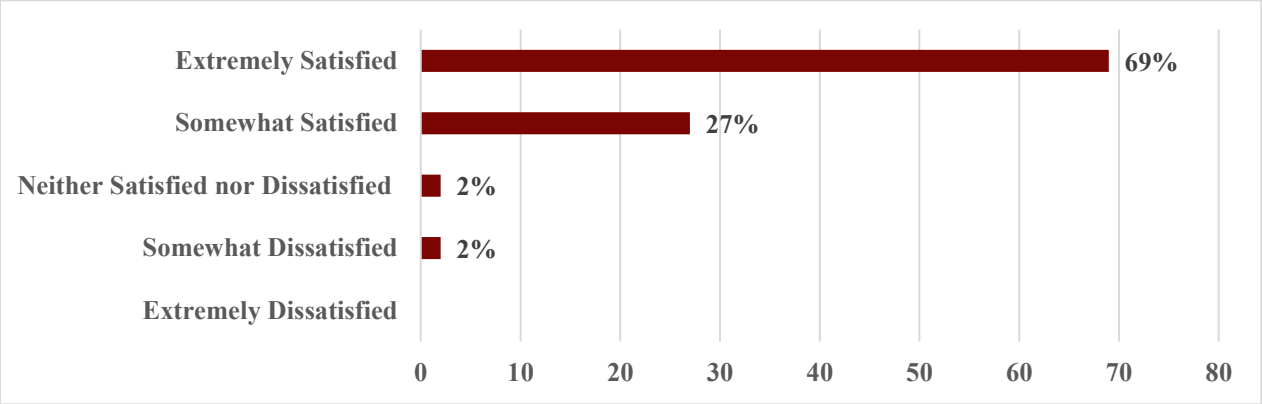
Participants' Perceived Satisfaction:

As part of the post-seminar evaluation, participants were asked to rate their overall satisfaction with the Spring 2025 seminar series using a five-point scale ranging from *extremely dissatisfied* to *extremely satisfied*.

- 69% rated being *extremely satisfied*
- 27% reported *somewhat satisfied*
- 2% indicated their satisfaction as *neutral (neither satisfied nor dissatisfied)*
- 2% rated being *somewhat dissatisfied*

The findings indicate a consistently high level of satisfaction among participants.
(See Figure 8. Participants' Perceived Satisfaction for the Spring 2025 Seminar Series).

Figure 8. Participants' Perceived Satisfaction for the Spring 2025 Seminar Series



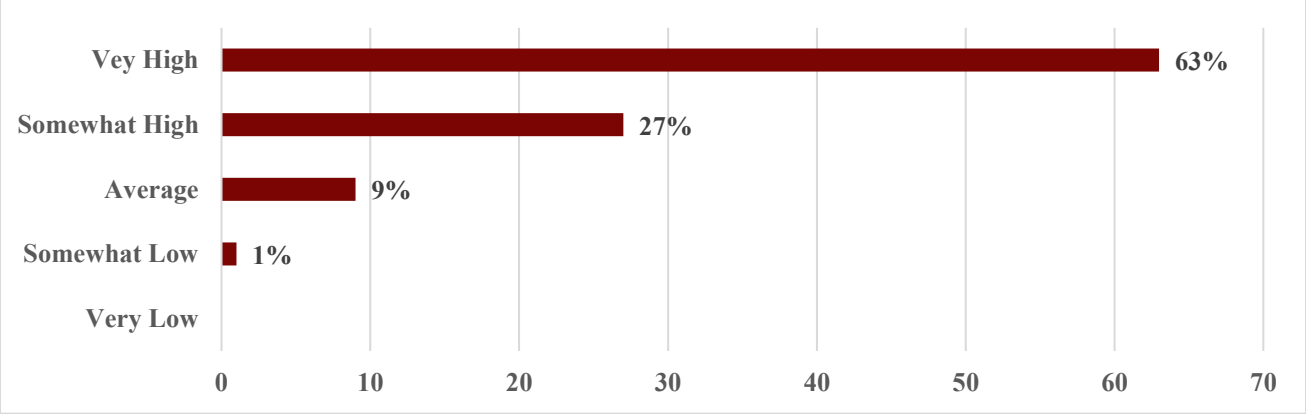
Seminars' Effectiveness in Promoting Learning:

Participants also evaluated the seminar's effectiveness in enhancing their understanding of cybersecurity concepts. Using a scale ranging from *very low* to *very high*, participants provided the following ratings:

- 63% rated the seminars as having *very high effectiveness*
- 27% indicated *somewhat high effectiveness*
- 9% rated them as *average*
- 1% reported *somewhat low effectiveness*

These results indicate that the majority of attendees found the seminars to be highly effective in promoting learning and comprehension of cybersecurity topics. (Table 9 presents participants' perceptions of the seminars' effectiveness).

Figure 9. Participants' Perceived Effectiveness for the Spring 2025 Seminar Series



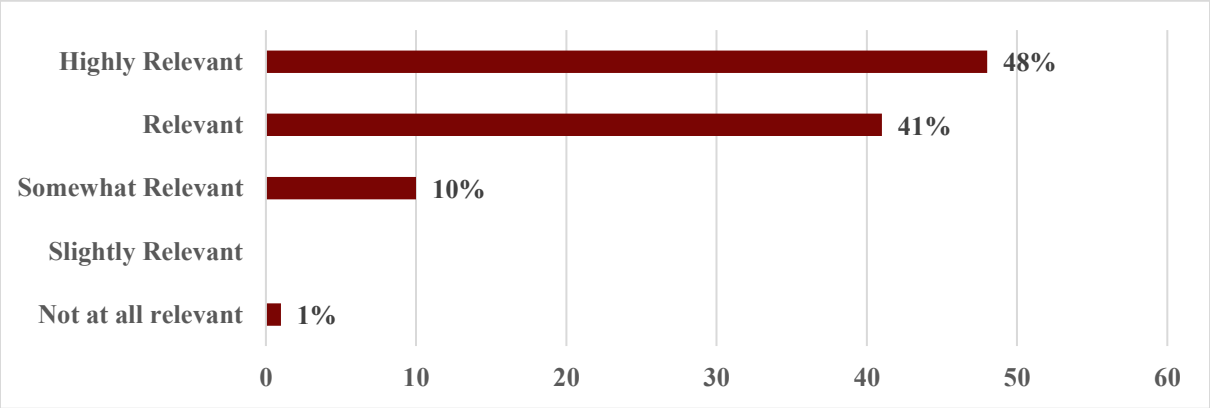
Seminars' Relevance to Participants' Need or Interest

Participants were also asked to assess the relevance of the Spring 2025 seminar topics and activities in relation to their academic or professional interests. Using a scale from *not at all relevant* to *highly relevant*, the distribution of responses was as follows:

- 48% rated the content as *highly relevant*
- 41% indicated it was *relevant*
- 10% selected *somewhat relevant*
- 1% indicated the content was *not at all relevant*

These results suggest that the seminar series was broadly aligned with the interests and developmental needs of its audience. (See Figure 10. Participants' Perceived Relevance for the Spring 2025 Seminar Series).

Figure 10. Participants' Perceived Relevance for the Spring 2025 Seminar Series



Positive Feedback:

Across all six Spring 2025 seminar sessions, participant responses reflected a high degree of engagement and satisfaction. The feedback emphasized several strengths of the seminar design and delivery. Participants particularly appreciated the use of visual aids, including diagrams and graphs, which enhanced their understanding of abstract or technical concepts. Participants found the sessions engaging, with several noting that presenters were effective in scaffolding the content, starting with basic principles and then delving deeper. Additionally, students valued the career presentations, such as the Scholarship for Service (SFS) program overview, internship opportunities, and insights into professional cybersecurity roles.

Direct Quotes from Participants:

- *"The information was very informative and relevant to present-day issues. It was simple enough for those who may not have a strong background in computer science to understand while still hitting the important points relating to cybersecurity."*
- *"I liked how she not just conveyed her slides but also formatted them to be interesting to look at with clear diagrams, images, and colors."*
- *"I liked hearing about the general overview of SFS Program. It was very informative and, of course, relevant to us students."*

This feedback underscores the seminars' success in combining accessible instruction with meaningful professional development content.

Need for Improvements:

While participants generally found the seminar series informative and well-presented, some had difficulty with the technical depth, such as understanding advanced graphs, acronyms, and detailed concepts that exceeded their knowledge. A few noted occasional audio issues, which affected their ability to remain fully engaged. This highlights the need for the program to include more explanations of technical content, consistent audio quality, and additional contextual support, such as real-world examples and simplified visuals, to enhance comprehension and engagement for a broader range of participants.

Direct Quotes from Participants:

- *"I thought there could have been a bigger focus on the cybersecurity side of it and less of the technicalities of the chemical processing side."*
- *"I found the methods of assessing critical facility power outage vulnerabilities challenging to understand due to my lack of knowledge in this field."*
- *"Only one small audio issue, but otherwise a great presentation."*

These comments offer valuable insights for improving future seminar design by emphasizing clarity, inclusivity, and instructional support across varying levels of expertise.

Cybersecurity Education and Research Summer 2025 Workshop

The workshop provided training that integrated cybersecurity research and education with professional teamwork, communication, leadership, and lifelong experiential learning. It included a variety of presentations, lectures, career development sessions, and hands-on activities focused on cybersecurity topics. Additionally, the workshop incorporated two field trips to Schweitzer Engineering Laboratories (SEL) in Pullman and Moscow.

Method

To evaluate the effectiveness of the workshop, the external evaluators administered a post-workshop survey using Qualtrics. The survey aimed to capture participants' perceptions of the workshop content, instructional delivery, and overall experience. Data were collected on the final day of the workshop and included both Likert-scale and open-ended questions (20 items total; see Appendix B for survey instrument). There was an average of 25 participants in each workshop session. Twenty participants (n = 20) completed the survey. Demographic data from survey respondents indicated the following:

- Participants' majors: Computer Science (n = 7), Cybersecurity (n = 5), Management Information Systems (n = 4), History (n = 1), Chemical Engineering (n = 1), Psychology (n = 1), and Unknown (n = 1).
- Gender: 80% Male, 20% Female.
- Ethnicity: 65% identify as White/Caucasian, 15% as Asian, 10% as Black/African American, 5% as Native Hawaiian or Pacific Islander, and 5% as other.

(Refer to Figures 11 and 12 for graphical representations of participants' gender and ethnicity).

Figure 11. Summer 2025 Workshop Participants' Gender

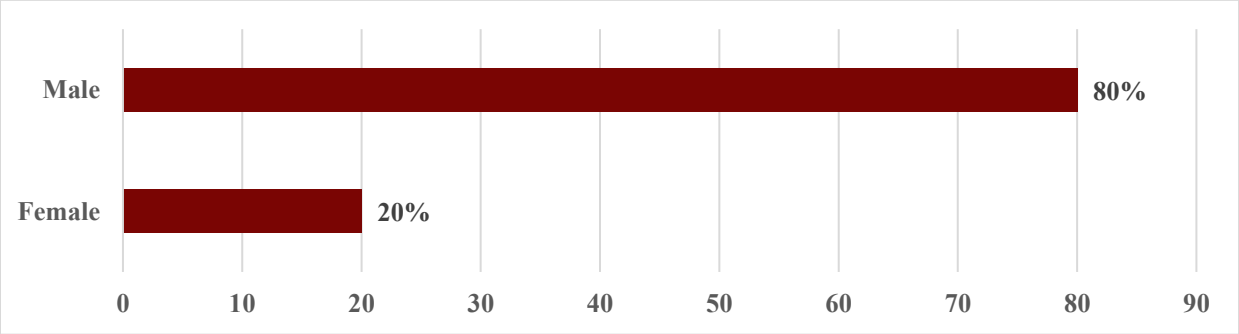
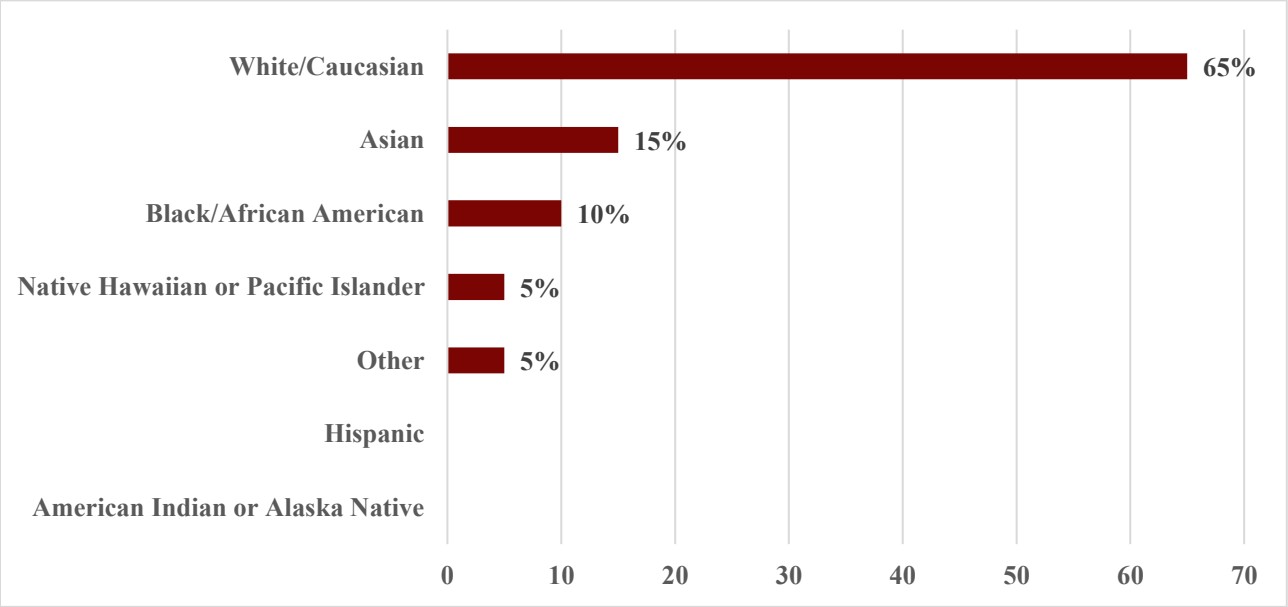


Figure 12. Summer 2025 Workshop Participants' Ethnicity



Activity Implementations and Key Findings

The workshop activities were designed to foster experiential learning while remaining aligned with the program's overarching goals.

Activity for Workshop:

The workshop was held in person, with the option for virtual participation. The following activities/lectures took place during the workshop:

- Introductions
- Keynote Address
- Cybersecurity Education in the United States
- Operations and Opportunities at NUWC Keyport
- Protecting Against Digital Repression
- Towards Usable and Practical Image Privacy
- Verifications Using Software Contracts
- Web Security and Privacy
- Incident Commander's Guide to Cybersecurity Strategy Cybersecurity Industry Panel Discussion - PNNL
- Securing AI: Think Outside the LLM - PNNL
- A Framework for Automatic Mapping of Vulnerabilities to Attack Patterns using Artificial Intelligence – PNNL
- Quantum Computing Overview
- Post-Quantum Cryptography

- Security of Time-Series Machine Learning
- Getting the Most from Your Internships
- Life-Long Learning and Professional Development
- Hands-on Demo on Cyber-Physical Systems Security
- Hands-on Demo on Digital Forensics
- Cybersecurity Industry Panel Discussion

In addition to various presentations, the workshop included opportunities for students to showcase their work through 12 poster presentations. Certificates were also awarded to acknowledge various accomplishments. In addition, the two field trips enhanced experiential learning and practical knowledge.

Sub Activity 1-1:

As part of the Summer 2025 CySER Workshop, participants engaged in several culminating activities that showcased their learning and fostered community engagement. These included:

- Student Poster Presentations, in which participants shared insights from their learning and collaborative projects.
- A Certificate Ceremony recognizing CySER graduates for their successful completion of the program.
- Two field trips to Schweitzer Engineering Laboratories (SEL) in Pullman and Moscow, offering students direct exposure to real-world cybersecurity practices in industry settings.

Key Findings

Survey responses from workshop participants were analyzed using descriptive statistics to assess the overall impact of the workshop experience.

- 61% of respondents indicated they learned a great deal or a lot from participating in the workshop.
- 28% reported moderate learning through experiential activities.
- 11% indicated they experienced little learning in relation to cybersecurity concepts.

These findings suggest that the majority of participants found the workshop to be highly effective in promoting meaningful engagement and knowledge acquisition. The combination of applied learning opportunities, industry interaction, and recognition of achievement appears to have contributed positively to the participants' educational experience.

Response to topics/activities during the workshop:

The first part of the post-workshop survey assessed participants' perceived learning across the various sessions and activities offered during the summer 2025 CySER Workshop. Participants were asked to indicate the extent to which they learned from each topic, with response options ranging from *very little* to *a great deal.*

High-Rated Learning Topics (≥70%)

A majority of participants (70% or more) indicated that they learned *a lot* or *a great deal* from the following sessions, signaling their effectiveness in conveying cybersecurity concepts:

- *Towards Usable and Practical Image Privacy* (75%)
- *Cybersecurity Education in the United States* (70%)
- *Incident Commander's Guide to Cybersecurity Strategy – PNNL* (70%)
- *Life-Long Learning and Professional Development* (70%)
- *Securing AI: Think Outside the LLM – PNNL* (70%)
- *Protecting Against Digital Repression* (70%)
- *Hands-on Demo on Digital Forensics* (70%)
- *Hands-on Demo on Cyber-Physical Systems Security* (70%)
- *Web Security and Privacy* (70%)

These results underscore the value of applied hands-on sessions and practical cybersecurity insights in supporting deep learning among participants.

Moderately Rated Topics (50 -69%)

The following sessions received moderately strong learning ratings, with 50% to 69% of participants reporting that they learned *a lot* or a *great deal*:

- *Verification Using Software Contracts* (65%)
- *Operations and Opportunities at NUWC Keyport* (60%)
- *Keynote Address* (55%)
- *Getting the Most from Your Internships* (55%)
- *Introductions* (50%)
- *A Framework for Automatic Mapping of Vulnerabilities to Attack Patterns Using Artificial Intelligence – PNNL* (50%)

While generally well-received, these topics may benefit from the inclusion of more interactive components or real-world demonstrations to further enhance comprehension and application.

Lower-Rated Topics (40–49%)

Three sessions received relatively lower ratings, with fewer than half of the participants reporting significant learning gains:

- *Quantum Computing Overview* (45%)
- *Post-Quantum Cryptography* (45%)
- *Security of Time-Series Machine Learning* (40%)

These findings suggest that topics involving advanced theoretical or emerging technical content may require additional scaffolding or instructional support to ensure accessibility, especially for learners with limited prior exposure.

Conclusion and Recommendations

Overall, the data indicate that participants responded most positively to career-focused, hands-on, and practically oriented sessions. These findings support the continued inclusion of such components in future CySER programming. It is strongly recommended that educators, policymakers, and program designers continue to prioritize interactive learning opportunities and real-world applications to sustain student engagement and enhance learning outcomes in cybersecurity education.

Response to Activity Relating to Field Trips:

As part of the Summer 2025 CySER Workshop, participants attended field trips to Schweitzer Engineering Laboratories (SEL) in both Pullman and Moscow, providing a unique opportunity to observe cybersecurity applications in real-world industrial contexts. Survey results revealed that 88% of respondents reported the field trips significantly enhanced their learning experience, stating they learned *a lot* or *a great deal* from the site visits. This finding highlights the value of immersive, industry-based learning in reinforcing theoretical content and contextualizing cybersecurity practices.

Measuring the Effectiveness of the Workshop:

To assess the overall impact of the workshop, participants were asked to evaluate the effectiveness of key components—including presentations, lectures, field trips, poster sessions, and hands-on activities—in promoting their understanding of cybersecurity. Responses were collected using a five-point Likert scale, ranging from *very low* to *very high effectiveness.*

The results below summarize participants' perception of somewhat or very high effectiveness:

- Hands-on demonstrations – 95% rated as somewhat or very high effectiveness
- Field trips – 95% rated as somewhat or very high effectiveness
- Industry panel – 90% rated as somewhat or very high effectiveness
- Poster presentations – 65% rated as somewhat or very high effectiveness

- Lectures – 60% rated as somewhat or very high effectiveness
- Overall workshop effectiveness – 81% rated the workshop activities as somewhat or very high effectiveness in enhancing cybersecurity learning.

These findings underscore that experiential and applied learning formats, such as demonstrations and field-based exposure, were most impactful. Conversely, more passive components, such as poster sessions and lectures, were perceived as less effective and may benefit from additional interactivity or scaffolding in future iterations.

Also, participants were asked to rate the value they received, considering the time spent attending the workshop. A significant majority, 90% of the respondents, indicated that the workshop was valuable to their learning experience and time spent attending it.

Findings on Key Things Learned from the Workshop:

To assess the alignment of the workshop with participants' academic and professional goals, attendees were asked to respond to a set of open-ended questions. The responses provided rich insights into the perceived value, impact, and learning outcomes gained from the Summer 2025 CySER Workshop.

Broadened Understanding of Cybersecurity

Many participants emphasized that the workshop significantly expanded their conceptualization of cybersecurity, particularly through exposure to its multidisciplinary nature and real-world implications. As one participant noted:

"Cybersecurity is an amazingly broad field and is made up of many facets."

Others highlighted how the workshop helped bridge the gap between academic coursework and professional practice:

"It's reassuring to know that the ideas I take away from class are also applied to real-world issues."

Participants also came away with a deeper appreciation for the physical dimension of cybersecurity, as reflected in this comment:

"I learned that cybersecurity effects aren't only digital but also physical."

Impact of Field Trips and Hands-On Activities

Several participants pointed to field trips and demonstrations as the most impactful elements of the workshop. These experiential components not only deepened technical understanding but also provided industry exposure:

"I appreciated learning how circuit boards are created at the SEL tour."

"One of my best life experiences was this workshop—it may even be career altering."

Career Preparation and Professional Growth

Participants consistently praised the career development content, including sessions on internships, industry panels, and networking. These activities helped them formulate concrete steps toward career advancement:

"Making the most of my internships, developing goals before arriving, was something I gained from this workshop."
"I was able to learn about the industry, what to do at internships, and how to focus in on a specific topic."
"Learn how to network, and have a roadmap to securing an internship."
"Cybersecurity is as much about who you work with as what you work on."

Overall Alignment with Participant Goals

Taken together, participants' reflections indicate that the workshop's structure, content, and delivery were well-aligned with their academic and professional objectives. The integration of technical knowledge, applied practice, and career exploration proved especially effective in enhancing learning and motivation.

Overall Feedback on the Workshop Satisfaction

To evaluate the breadth and quality of content offered, participants were asked to rate their satisfaction with the variety of topics presented during the Summer 2025 CySER Workshop. The responses indicate uniformly positive perceptions:

- A majority of the participants reported being either *satisfied* or *somewhat satisfied* with the diversity of topics covered.
- A majority expressed that they were strongly satisfied with the range and relevance of the subjects addressed.

In addition to the variety of topics, participants expressed overall satisfaction with the content quality, presentations, field trips, and lectures. Feedback suggests that the structure, delivery, and balance of technical depth and professional development met or exceeded participant expectations.

These findings affirm the comprehensive design and participant-centered approach of the workshop, underscoring its success in delivering a meaningful and engaging educational experience.

Suggestions for How Future Workshops Could be Improved:

Most participants strongly agreed that the workshop sessions facilitated their learning experience in cybersecurity education and research. However, the following suggestions were made to improve the learning experience in future workshops.

1. More hands-on activities during the lecture-style presentations
2. More opportunities for hands-on activities throughout the workshop
3. More collaborative sessions during learning activities
4. More time for breaks and healthy snack options in the mornings.

Direct Quotes from Participants:

- *"More hands-on mixed in with the lectures."*
- *"I really liked the hands-on demos and would've liked more time for that."*
- *"Possibly more hands-on group learning."*
- *"Longer breaks in between speakers (I have ADHD)."*
- *"The only thing I'd improve is to add a little bit more time to the lunch breaks. Maybe 10-20 minutes more just in case some of us want to go back home and eat something."*
- *"A healthier choice of snacks in the morning" and "more time for lunch break."*

Most participants recommended introducing more hands-on activities, group sessions, and longer breaks in future workshops.

Recommendations for future workshops

We commend the principal investigators and key personnel for their exemplary implementation of the Summer 2025 CySER Workshop. Notably, many of the recommendations from the previous year were effectively integrated into this year's program design. Participant feedback and survey results consistently affirm the workshop's impact and effectiveness in advancing cybersecurity education and research.

To further enhance the learning experience and program effectiveness in future iterations, the following recommendations are offered:

1. Integrate More Hands-On Learning Within Lectures:
   Supplement lecture-style presentations with interactive, hands-on activities that allow participants to apply theoretical concepts in real time. This will deepen understanding and promote knowledge retention.
2. Expand Career Development Components: Continue to offer and expand sessions focused on cybersecurity career pathways, internships, and industry engagement. These elements are instrumental in fostering students' motivation and professional readiness.

3. Promote Peer Collaboration Opportunities: Incorporate structured collaborative activities or group-based sessions to foster peer-to-peer learning engagement. These opportunities can enhance networking, teamwork skills, and interdisciplinary problem-solving.
4. Incorporate Additional Break Time Between Sessions: Introduce longer or more frequent breaks between sessions to sustain participant focus, reduce cognitive fatigue, and support overall workshop engagement and well-being.

By implementing these strategies, future workshops can continue to build on CySER's success and further enrich participants' academic and professional development in cybersecurity.

Conclusion:

CySER continues to make significant contributions toward building a diverse and skilled cybersecurity workforce. This year's evaluation findings affirm the program's success in delivering high-impact learning experiences and positioning students for future leadership in cybersecurity. With continued innovation and responsive improvements, CySER is well-positioned to sustain its regional and national impact in cybersecurity education and research.

Appendix A

Thank you for attending this seminar and for taking the time to leave feedback about your experience. This survey will take approximately 10 minutes.

Q1 Overall, how satisfied were you with the seminar?

- ❍ Extremely satisfied
- ❍ Somewhat satisfied
- ❍ Neither satisfied nor dissatisfied
- ❍ Somewhat dissatisfied
- ❍ Extremely dissatisfied.

Q2 Overall, how would you rate the effectiveness of today's seminar in promoting your learning about cybersecurity concepts?

- ❍ Very high
- ❍ Somewhat high
- ❍ Average
- ❍ Somewhat low
- ❍ Very low

Q3 How would you rate the overall quality of the seminar?

- ❍ Excellent
- ❍ Good
- ❍ Fair
- ❍ Poor
- ❍ Very poor

Q4 How relevant was the seminar content to your needs or interests?

- ❍ Highly relevant
- ❍ Relevant
- ❍ Somewhat relevant
- ❍ Slightly relevant
- ❍ Not at all relevant

Q5 What aspect(s) of the seminar did you find particularly helpful?

_____

_____

_____

Q6 What aspect(s) of the seminar did you find least effective or most challenging and why??

_____

_____

_____

_____

Q7 Was the seminar engaging and interactive

- ❍ Strongly agree
- ❍ Somewhat agree
- ❍ Neither agree nor disagree
- ❍ Somewhat disagree
- ❍ Strongly disagree

Q8 How effective was the presenter in delivering the content?

- ❍ Very effective
- ❍ Effective
- ❍ Neutral
- ❍ Ineffective
- ❍ Very ineffective

Q9 What types of Seminars do you want to see in the future?

- ❍ Career Information
- ❍ Research-based cybersecurity concepts
- ❍ Hybrid – Career and Research-based cybersecurity concepts
- ❍ Others

Q10 Identify three key things you learned from this seminar.

_____

_____

_____

_____

Q11 Please provide any additional comments or suggestions for future seminars.

_____

_____

_____

_____

Q12 Please provide the name of your university

_____

Q13 What is your current status or position at the school?

- ❍ Freshman (1st year)
- ❍ Sophomore (2nd year)
- ❍ Junior (3rd year)
- ❍ Senior (4th year)
- ❍ Graduate student (Master's)
- ❍ Doctoral student (PhD)
- ❍ Postdoctoral Fellow
- ❍ Faculty
- ❍ Staff
- ❍ Other

Q14 What is your gender?

- ❍ Male
- ❍ Female
- ❍ Other (please identify)
- ❍ Prefer not to say

Q15 What do you identify as your ethnicity?

- ☐ White/Caucasian
- ☐ Black or African American
- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Native Hawaiian or Pacific Islander
- ☐ Hispanic
- ☐ Other

Appendix B

Cybersecurity Education & Research Summer Workshop 2025

Thank you for participating in the 2025 Cybersecurity Education and Research Summer Workshop. This brief survey is designed to gather your feedback about the workshop's content, delivery, and overall impact. It will take approximately 20 minutes to complete. Your responses will be kept confidential, and only summarized aggregate results will be used for evaluation and reporting purposes.

We greatly appreciate your time and valuable input.

Q1 On a scale of 1 to 5 (none at all .... a great deal), how would you rate how much you learned each of these topics as a result of attending this workshop?

	None at all	A little	A moderate amount	A lot	A great deal
Introduction	❍	❍	❍	❍	❍
Keynote Address	❍	❍	❍	❍	❍
Cybersecurity Education in the United States	❍	❍	❍	❍	❍
Operations and Opportunities at NUWC Keyport	❍	❍	❍	❍	❍
Protecting Against Digital Repression	❍	❍	❍	❍	❍
Towards Usable and Practical Image Privacy	❍	❍	❍	❍	❍
Verifications Using Software Contract	❍	❍	❍	❍	❍

Q2 On a scale of 1 to 5 (none at all .... a great deal), how would you rate how much you learned each of these topics as a result of attending this workshop?

	None at all	A little	A moderate amount	A lot	A great deal
Web Security and Privacy	❍	❍	❍	❍	❍

Incident Commander's Guide to Cybersecurity Strategy - PNNL	❍	❍	❍	❍	❍
Securing AI: Think Outside the LLM - PNNL	❍	❍	❍	❍	❍
A Framework for Automatic Mapping of Vulnerabilities to Attack Patterns using Artificial Intelligence - PNNL	❍	❍	❍	❍	❍

Q3 On a scale of 1 to 5 (none at all .... a great deal), how would you rate how much you learned each of these topics as a result of attending this workshop

	None at all	A little	A moderate amount	A lot	A great deal
Quantum Computing	❍	❍	❍	❍	❍
Post-Quantum Cryptography	❍	❍	❍	❍	❍
Security of Time Series Machine Learning	❍	❍	❍	❍	❍
Getting the Most from your Internships	❍	❍	❍	❍	❍
Life-Long Learning and Professional Development	❍	❍	❍	❍	❍

Q4 On a scale of 1 to 5 (none at all .... a great deal), to what extent did each of the hands-on activities help you learn in this workshop?

	None at all	A little	A moderate amount	A lot	A great deal
Hands-on Demo on Cyber-physical Systems Security	❍	❍	❍	❍	❍
Hands-on Demo on Digital Forensics	❍	❍	❍	❍	❍

Q5 On a scale of 1 to 5 (none at all .... a great deal), to what extent did the field trip and outings enhance your experience?

	None at all	A little	A moderate amount	A lot	A great deal
Schweitzer Engineering Labs (SEL) - Pullman	❍	❍	❍	❍	❍
Schweitzer Engineering Labs (SEL) - Moscow	❍	❍	❍	❍	❍

Q6 To what extent did industry panel discussions enhance your experience of the cybersecurity industry?

- ❍ Very high
- ❍ Somewhat high
- ❍ Average
- ❍ Somewhat low
- ❍ Very low

Q7 To what extent did industry panel discussions enhance your understanding of the cybersecurity industry?

- ❍ Very high
- ❍ Somewhat high
- ❍ Average
- ❍ Somewhat low
- ❍ Very low

Q8 To what extent did the poster presentations enhance your experience of cybersecurity concepts?

- ❍ Very high
- ❍ Somewhat high
- ❍ Average
- ❍ Somewhat low
- ❍ Very low

Q9 To what extent did the poster presentations enhance your understanding of cybersecurity concepts?

- ❍ Very high
- ❍ Somewhat high
- ❍ Average

- ❍ Somewhat low
- ❍ Very low

Q10 Overall, how would you rate the effectiveness of the following components in promoting your learning about cybersecurity? Please select one option per row.

	Very High	Somewhat High	Average	Somewhat Low	Very Low
Lectures	❍	❍	❍	❍	❍
Poster Presentations	❍	❍	❍	❍	❍
Hands on Demonstration	❍	❍	❍	❍	❍
Field Trips	❍	❍	❍	❍	❍
Industry Panel	❍	❍	❍	❍	❍

Q11 Considering the total time invested, how would you rate the overall value you received from the workshop?

- ❍ Very high
- ❍ Somewhat high
- ❍ Average
- ❍ Somewhat low
- ❍ Very low

Q12 What are three most important things you learned from this workshop?

_____

_____

_____

_____

Q13 Could you please explain how those things you learned align (or not) with your goals for the workshop?

_____

_____

_____

Q14 Please share your suggestions for how future workshops could be improved.

_____

_____

_____

_____

Q15 Overall, how satisfied are you with the variety of topics presented at this workshop?

- Very satisfied
- Somewhat satisfied
- Neither satisfied nor dissatisfied
- Somewhat dissatisfied
- Strongly dissatisfied.

Q16 My name is

_____

Q17 Please enter your program level.

- Undergraduate
- Masters
- Doctoral - PhD
- Faculty
- Other

Q18 If undergrad, my major is:

_____

Q19 I am a

- ❍ Male (1)
- ❍ Female (2)
- ❍ Other (3)

Q20 What do you identify as your ethnicity?

- ☐ White/Caucasian
- ☐ Black or African American
- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Native Hawaiian or Pacific Islander
- ☐ Hispanic
- ☐ Other

Before you submit, you can modify your answers by clicking the “Back” function Once you click “Next” your responses will be finalized and cannot be changed.