

VICEROY Northwest Institute for Cybersecurity Education and Research (CySER)

Evaluation Report Year 5

Prepared for:

Dr. Assefaw Gebremedhin

Dr. James Crabb

Prepared by:

Blessing Akinrotimi

Dr. Oluwafemi Sunday

Dr. Olusola Adesope



Table of Contents

<i>EXECUTIVE SUMMARY</i>	4
Summary of Findings.....	4
Summary of Recommendations	4
<i>BACKGROUND AND CONTEXT</i>	5
VICEROY Initiative and CySER.....	5
Program Components.....	5
<i>EVALUATION OVERVIEW</i>	6
Evaluation Purpose	6
Evaluation Methods	6
Data Sources	6
Participants.....	6
Data Analysis	6
Evaluation Outcome Achievements (August 2025 – May 2026).....	7
<i>2025 FALL SEMINAR SERIES</i>	8
Methods	8
Key Findings.....	9
Perceived Satisfaction	9
Perceived Effectiveness	9
Perceived Engagement.....	10
Perceived Relevance	11
Perceived Quality	12
Positive Experiences	13
Areas for Improvement	14
<i>2026 SPRING SEMINAR SERIES</i>	16
Methods	16
Key Findings.....	17
Perceived Satisfaction	17
Perceived Effectiveness	18
Perceived Engagement.....	19
Perceived Relevance	20
Perceived Quality	21
Positive Experiences	22
Areas for Improvement	23
Recommendations for Future Seminars.....	25
<i>2026 CYBERSECURITY EDUCATION AND RESEARCH SUMMER WORKSHOP</i>	26
Activity Implementations.....	26

Presentations	26
Hands-on Activities.....	26
Field Trips	27
Industry Panel	27
Student Panel	27
Poster Session	27
Methods	28
Key Findings.....	28
Response to topics/hands-on during the workshop:.....	28
Response to Activity Relating to Field Trips	29
Response to Activity Relating to Poster Presentations and Panels	30
Measuring the Effectiveness of the Workshop.....	30
Findings on Key Things Learned from the Workshop	30
Recommendations for Future Workshops	31
Conclusion	32
Appendix A: 2026 Fall/Spring Seminar Survey	33
Appendix B: 2026 CySER Summer Workshop Survey	36

EXECUTIVE SUMMARY

The VICEROY Northwest Institute for Cybersecurity Education and Research (CySER) is a Department of Defense (DoD) funded program established to train the next generation of the military and national defense-aligned civilian workforce in cybersecurity. CySER integrates cybersecurity research and education with professional skills in teamwork, communication, leadership, and lifelong learning. Core program elements include virtual seminars during the academic year, capstone projects, competitions, research projects, an annual summer workshop, and internship opportunities at DoD installations, national laboratories, and cybersecurity industry partners.

Evaluation is an integral component of the CySER program. This evaluation was prepared by the external evaluation team and covers the fall 2025 and spring 2026 seminar series, and the 2026 CySER Summer Workshop. The evaluation employed a descriptive design, using post-seminar and workshop surveys administered through Qualtrics. On average, 17 participants completed each fall 2025 seminar survey and 10 completed each spring 2026 seminar survey; 14 participants completed the workshop survey. Data were analyzed using descriptive statistics for closed-ended items and thematic analysis for open-ended responses. The purpose of this evaluation 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.

Summary of Findings

1. Participants across both seminar series and the summer workshop reported consistently high levels of satisfaction, engagement, and perceived learning.
2. Participants preferred seminar and workshop formats that combined career development content with research-based cybersecurity concepts.
3. Hands-on activities and field trips emerged as the most highly rated components of the workshop.
4. Participants reported that the workshop strengthened their interest in cybersecurity careers and fostered meaningful peer connections.
5. Participants identified pacing, technical complexity, and content accessibility as recurring areas for improvement across both the seminar series and the summer workshop.

Summary of Recommendations

1. Sustain and expand the hybrid seminar format that integrates career development with research-based cybersecurity content.
2. Expand hands-on and field trip learning opportunities at future summer workshops, as they were rated as the most effective components of the workshop.
3. Increase scaffolding of technical content for participants with limited prior knowledge in a complex topic area.
4. Develop more structured and intentional networking opportunities for participants.
5. Diversify the range of industry sectors represented in presentations and panel discussions.

BACKGROUND AND CONTEXT

VICEROY Initiative and CySER

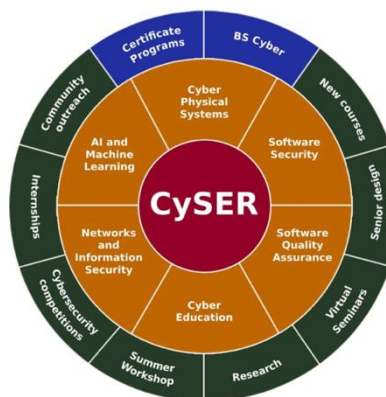
Washington State University established the VICEROY Northwest Institute for Cybersecurity Education and Research (CySER) to address a critical national need by preparing a highly skilled cybersecurity workforce aligned with military and national defense priorities. CySER is funded through the DoD Virtual Institutes for Cyber and Electromagnetic Spectrum Research and Employ (VICEROY) initiative, operated by the Griffiss Institute in collaboration with the Air Force Research Laboratory. The VICEROY initiative supports innovative cybersecurity education and research programs for ROTC cadets and DoD-aligned civilians at the undergraduate level. CySER is a consortium of four institutions in the Pacific Northwest, led by Washington State University (WSU). The other three partner institutions are Montana State University (MSU), the University of Idaho (UI), and Central Washington University (CWU). In the first two years of the program, Columbia Basin College (CBC) also participated as a consortium member.

Program Components

CySER responds to the VICEROY initiative by designing an innovative education and research program that integrates theoretical knowledge with experiential learning. The program prepares students in technical cybersecurity domains and in professional skills, including teamwork, communication, leadership, and lifelong learning. CySER's research spans six focus areas: AI and Machine Learning, Cyber-Physical Systems, Networks and Information Security, Software Security, Software Quality Assurance, and Cyber Education. See Figure 1 for CySER's components and topic areas. The key program elements are also listed below:

- **Virtual Seminars:** Bi-weekly seminars during the academic year featuring expert presentations on research, current trends, and industry career pathways. Four seminars were held in the fall semester and six in the spring semester.
- **Annual Workshop:** The 2026 CySER Summer Workshop was held on the WSU Pullman campus, featuring presentations, hands-on activities, field trips, industry panels, student poster presentations, and certificate ceremonies.
- **Internships:** Placement opportunities at DoD-based installations, national laboratories, and cybersecurity industry partners.
- **New Courses and Capstone Projects:** Development of new cybersecurity courses and modules, as well as senior design and capstone projects with an applied cybersecurity focus.
- **Research:** Participation in research with mentorship from experts.
- **Cybersecurity Competitions:** Participation in national competitions such as the National Cyber League to develop applied skills.
- **Community Outreach:** Engagement with high school students and educators to build the cybersecurity pipeline.

Figure 1. CySER Components and Topics



EVALUATION OVERVIEW

Evaluation Purpose

The evaluation aims to provide useful information to CySER program coordinators, principal investigators, DoD, and Griffiss Institute VICEROY team members to guide program improvement, assess annual effectiveness, and support continued funding. The focus of this annual evaluation is on three program components: the fall 2025 and spring 2026 seminar series and the 2026 CySER Summer Workshop. The evaluation examines participants' learning experiences, perceived satisfaction and effectiveness, content relevance, engagement, and impact on career development across all three program components.

Evaluation Methods

The evaluation employed a descriptive approach, using surveys conducted via Qualtrics. Surveys included both closed-ended and open-ended questions designed to capture participants' experiences and perceptions. The closed-ended data were analyzed with descriptive statistics and presented as percentages to summarize responses across key dimensions, including satisfaction, effectiveness, quality, relevance, and engagement. Open-ended survey responses were analyzed deductively using the survey questions. The seminar surveys asked about positive experiences and areas for improvement. The workshop survey asked about key takeaways and suggestions for future workshops. All open-ended responses were reviewed by the evaluator, and recurring themes were identified across responses. Representative quotes were selected to illustrate the most common themes and are presented verbatim from participant responses.

Data Sources

The primary data source for this evaluation was post-surveys administered via Qualtrics. Two survey instruments were used: a seminar survey administered after each bi-weekly seminar and a workshop survey administered on the final day of the 2026 CySER Summer Workshop. The seminar survey consisted of 16 items assessing participants' overall satisfaction, effectiveness, seminar quality, content relevance, engagement, preferred future seminar formats, open-ended questions on key learnings and suggestions for improvement, and demographic items. The workshop survey comprised 17 items covering session-by-session learning ratings, activity effectiveness, open-ended questions on key learnings, and demographic items.

Participants

Across the fall 2025 seminar series, an average of 17 participants completed the post-seminar surveys, and an average of 10 participants completed the surveys in the spring 2026 seminar series. For the 2026 CySER Summer Workshop, 14 participants completed the post-workshop survey.

Data Analysis

Survey data were analyzed using descriptive statistics. For the closed-ended items, the frequency of respondents was calculated and reported as percentages. Findings were reported as the overall average across the seminar series and the individual seminar, based on respondents who completed the survey for that session. Responses to open-ended questions were reviewed to identify themes, and representative quotes were selected to illustrate key patterns in participant feedback. In addition to survey data, program documents were reviewed to highlight key

achievements for the 2025-2026 academic year. These documents included records of seminar topics and presenters, workshop activity logs, and summaries of key achievements. The key achievements from program documentation are presented in the section below.

Evaluation Outcome Achievements (August 2025 – May 2026)

Key achievements this funding year:

- A total of 10 seminars were delivered across two academic semesters - four in fall 2025 and six in spring 2026.
- The 2026 CySER Summer Workshop was successfully administered on the WSU Pullman campus, featuring 14 presentations, three hands-on activities, two field trips to Schweitzer Engineering Laboratories (SEL) in Pullman and Moscow, an industry panel, a student panel, and student poster presentations.
- CySER scholars earned first place at the 2026 VICEROY Competition held during this year's VICEROY Symposium.
- Thirteen students (12 WSU, 1 UI) were accepted for the VICEROY internships this year.
- Twenty-nine (25 WSU, 4 MSU) students were awarded certificates of participation in recognition of successfully completing their first year in the CySER program.
- The 2026 CySER Summer Workshop included 15 student poster presentations, representing research participated in by 26 students.
- In the Fall 2025 National Cyber League (NCL) season, WSU's Cybersecurity Group club competed across six teams, earning WSU 12th place in the NCL All College Power Rankings among more than 500 schools and 5th place among 50+ Western Colleges.
- In the VICEROY Shieldbearer Competition held November 4 to 6, 2025, WSU teams placed 3rd, 24th, 29th, 31st, and 38th out of 44 teams from across all VICEROY institutes.
- Industry partners, including Keyport Naval Undersea Warfare Center, Pacific Northwest National Laboratory, Schweitzer Engineering Laboratories, Fairchild Air Force Base, Idaho National Laboratory, Microsoft Corporation, and Mitre Corporation, continued to support the program through internships, site visits, or seminar presentations.
- The program continues to serve a diverse student population from all four consortium institutions with representation across gender, ethnicity, and academic level.

The following sections present detailed evaluation findings for the 2025-2026 CySER program year. Findings are organized by method and outcome for the Fall 2025 and Spring 2026 seminar series and the 2026 CySER Summer Workshop.

2025 FALL SEMINAR SERIES

The 2025 fall seminar series consisted of four expert and student-led presentations on applied topics in cybersecurity research, career development, and professional opportunity. The topics were as follows:

- Cyber-Physical System Recovery from Sensor Attacks – Dr. Mengyu Liu (WSU) - September 30, 2025.
- How Can Blockchain Enhance Trust in Digital Forensics and Evidence? – Dr. Asma Jodeiri Akbarfam (WSU) - October 14, 2025
- Post-Quantum Cryptography in Practice: From Standards to Systems – Dr. Ishaani Priyadarshini (WSU) - October 28, 2025
- CySER Student Experiences in VICEROY’s MAVEN and ENVOY Internships - Student Panel - November 18, 2025

Methods

After each seminar, a survey was administered online via Qualtrics. The survey comprised 16 questions assessing participants’ perceptions of satisfaction, effectiveness, seminar quality, content relevance, engagement, positive experience, areas for improvement, and demographic items (see appendix A for the survey instrument). Across the four fall 2025 seminars, an average of 17 participants completed the survey. Demographic data on the gender and ethnicity of survey respondents are presented below in Figures 2 and 3.

Figure 2. Fall 2025 Participants’ Gender

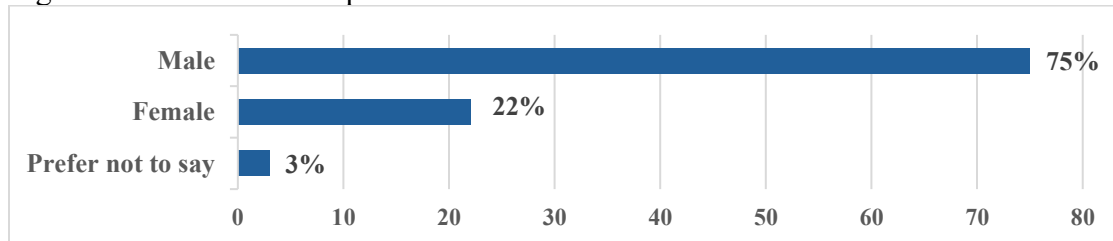
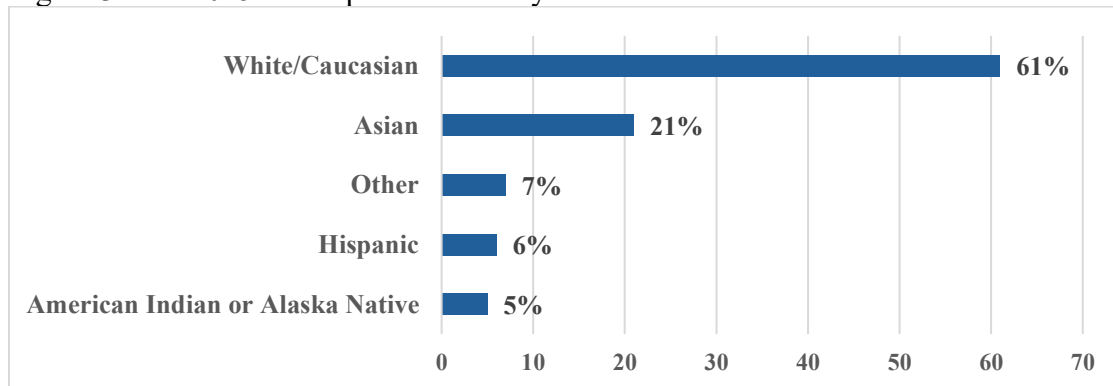


Figure 3. Fall 2025 Participants’ Ethnicity



Key Findings

Perceived Satisfaction

Participants rated their overall satisfaction with the fall 2025 seminar series on a scale from *extremely dissatisfied* to *extremely satisfied*. Overall, 64% of participants were extremely satisfied, 33% were somewhat satisfied, and 3% were neither satisfied nor dissatisfied. No participants reported being dissatisfied with the seminar series (see Figure 4 for participants' overall perceived satisfaction with the fall 2025 seminar series). Satisfaction ratings for each seminar provide a detailed view of participants' experiences across the fall 2025 seminar series, with the VICEROY Internship Experiences session recording the highest level of extreme satisfaction. The results, categorized by session, are as follows:

Seminar 1: Cyber-Physical System Recovery from Sensor Attacks

- 47% rated being extremely satisfied
- 40% reported being somewhat satisfied
- 13% indicated their satisfaction as neutral (neither satisfied nor dissatisfied)

Seminar 2: How Can Blockchain Enhance Trust in Digital Forensics and Evidence?

- 71% rated being extremely satisfied
- 29% reported being somewhat satisfied

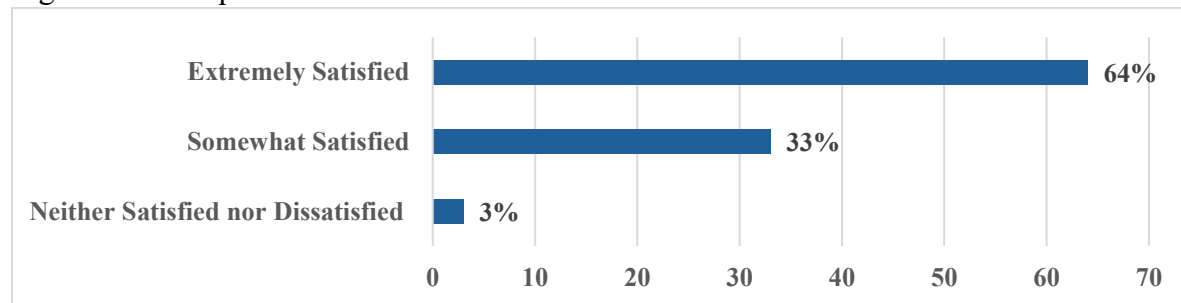
Seminar 3: Post-Quantum Cryptography in Practice: From Standards to Systems

- 56% rated being extremely satisfied
- 44% reported being somewhat satisfied

Seminar 4: CySER Student Experiences in VICEROY's MAVEN and ENVOY Internships

- 82% rated being extremely satisfied
- 18% reported being somewhat satisfied

Figure 4. Participants' Perceived Satisfaction for the Fall 2025 Seminar Series



Perceived Effectiveness

Participants rated the effectiveness of each seminar in promoting their understanding of cybersecurity concepts on a scale from *very low* to *very high*. Overall, 52% of participants rated the effectiveness as very high, 37% as somewhat high, and 11% as average. No participants rated the seminars as low or very low in effectiveness (refer to Figure 5 for participants' perceived

effectiveness of the fall 2025 seminar series). Effectiveness ratings for each seminar session provide a more nuanced understanding of participants' experiences across the fall 2025 seminar series, with the VICEROY Internship Experiences session recording the highest level of high effectiveness ratings among participants:

Seminar 1: Cyber-Physical System Recovery from Sensor Attacks

- 27% rated effectiveness as very high
- 53% rated it as somewhat high
- 20% rated it as average

Seminar 2: How Can Blockchain Enhance Trust in Digital Forensics and Evidence?

- 59% rated effectiveness as very high
- 35% rated it as somewhat high
- 6% rated it as average

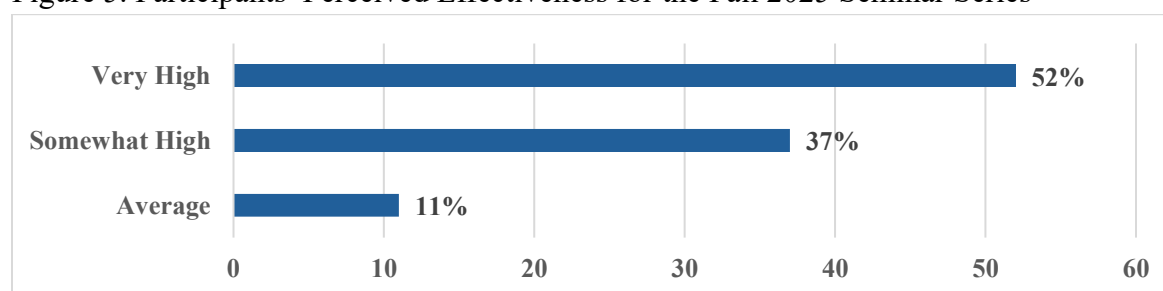
Seminar 3: Post-Quantum Cryptography in Practice: From Standards to Systems

- 56% rated effectiveness as very high
- 33% rated it as somewhat high
- 11% rated it as average

Seminar 4: CySER Student Experiences in VICEROY's MAVEN and ENVOY Internships

- 65% rated effectiveness as very high
- 29% rated it as somewhat high
- 6% rated it as average

Figure 5. Participants' Perceived Effectiveness for the Fall 2025 Seminar Series



Perceived Engagement

Participants rated the extent to which each seminar was engaging in promoting their learning about cybersecurity concepts on a scale from *strongly disagree* to *strongly agree*. Overall, 61% of participants strongly agreed that the seminars were engaging, 33% somewhat agreed, 5% neither agreed nor disagreed, and 1% somewhat disagreed (refer to Figure 6 for perceived engagement across the fall 2025 seminars). Engagement ratings for each seminar session provide a better understanding of participants' experiences across the fall 2025 seminar series, with the Blockchain and Digital Forensics session and the VICEROY Internship Experiences session recording the highest levels of strong agreement among participants:

Seminar 1: Cyber-Physical System Recovery from Sensor Attacks

- 53% strongly agreed that the seminar was engaging
- 33% somewhat agreed
- 14% neither agreed nor disagreed

Seminar 2: How Can Blockchain Enhance Trust in Digital Forensics and Evidence?

- 65% strongly agreed that the seminar was engaging
- 35% somewhat agreed

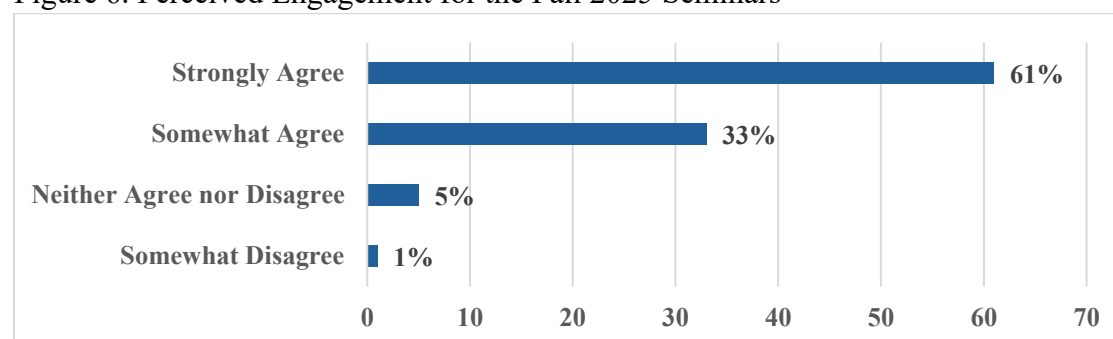
Seminar 3: Post-Quantum Cryptography in Practice: From Standards to Systems

- 61% strongly agreed the seminar was engaging
- 33% somewhat agreed
- 6% neither agreed nor disagreed

Seminar 4: CySER Student Experiences in VICEROY's MAVEN and ENVOY Internships

- 65% strongly agreed the seminar was engaging
- 29% somewhat agreed
- 6% somewhat disagreed

Figure 6. Perceived Engagement for the Fall 2025 Seminars



Perceived Relevance

Participants rated the relevance of each seminar to their interests on a scale from *not at all relevant* to *highly relevant*. Overall, 49% of participants rated the content as highly relevant, 43% rated it as relevant, 6% rated it as somewhat relevant, and 2% indicated the content was not at all relevant (see Figure 7 for participants' perceived relevance for the fall 2025 seminar series). Relevance ratings for each seminar session provide clearer insights into participants' experiences throughout the fall 2025 seminar series, with the VICEROY Internship Experiences session receiving the highest ratings:

Seminar 1: Cyber-Physical System Recovery from Sensor Attacks

- 26% rated the content as highly relevant
- 67% rated it as relevant
- 7% rated it as not at all relevant

Seminar 2: How Can Blockchain Enhance Trust in Digital Forensics and Evidence?

- 47% rated the content as highly relevant
- 41% rated it as relevant
- 12% rated it as somewhat relevant

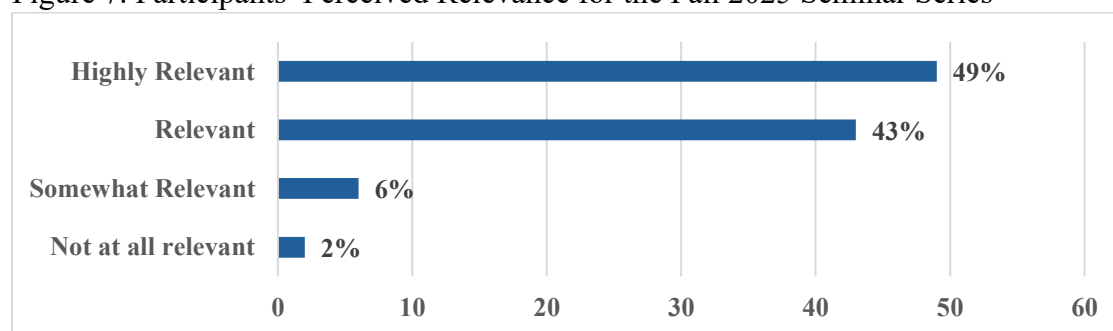
Seminar 3: Post-Quantum Cryptography in Practice: From Standards to Systems

- 44% rated the content as highly relevant
- 50% rated it as relevant
- 6% rated it as somewhat relevant

Seminar 4: CySER Student Experiences in VICEROY's MAVEN and ENVOY Internships

- 77% rated the content as highly relevant
- 17% rated it as relevant
- 6% rated it as somewhat relevant

Figure 7. Participants' Perceived Relevance for the Fall 2025 Seminar Series



Perceived Quality

Participants rated the overall quality of the fall 2025 seminar series on a scale from *very poor* to *excellent*. Overall, 55% rated the quality as excellent, 42% as good, and 3% as fair. No participants rated the seminars as poor or very poor in quality (see Figure 8 for participants' perceived seminar quality). Quality ratings for each seminar session provide a comprehensive understanding of participants' experiences across the fall 2025 seminar series, with the VICEROY Internship Experiences session recording the highest rates of excellent ratings among participants:

Seminar 1: Cyber-Physical System Recovery from Sensor Attacks

- 27% rated the quality as excellent
- 73% rated it as good

Seminar 2: How Can Blockchain Enhance Trust in Digital Forensics and Evidence?

- 65% rated the quality as excellent
- 35% rated it as good

Seminar 3: Post-Quantum Cryptography in Practice: From Standards to Systems

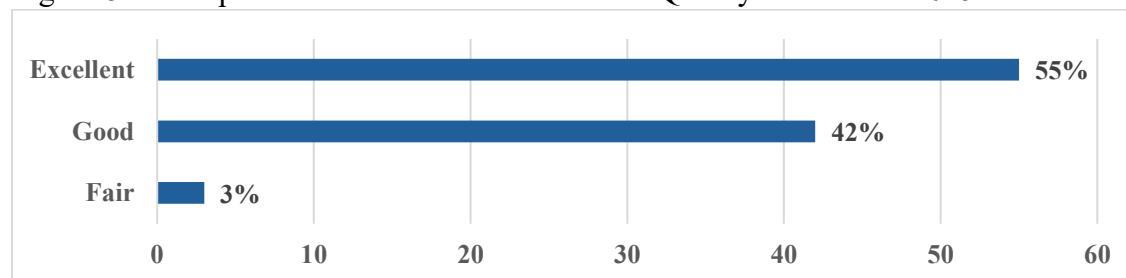
- 56% rated the quality as excellent
- 33% rated it as good

- 11% rated it as fair

Seminar 4: CySER Student Experiences in VICEROY's MAVEN and ENVOY Internships

- 71% rated the quality as excellent
- 29% rated it as good

Figure 8. Participants' Perceived Seminar Overall Quality for the Fall 2025 Seminar Series



Positive Experiences

Participants' open-ended responses were consistent with the high ratings for satisfaction, effectiveness, quality, relevance, and engagement reported across the fall 2025 seminar series, further highlighting positive learning experiences. Participants also expressed a continued preference for seminars that integrate career development content with research-based cybersecurity concepts.

In Seminar 1 on Cyber-Physical System Recovery, participants appreciated the use of real-world demonstrations and visual aids to make complex content accessible, highlighting the presenter's ability to connect technical concepts to everyday applications:

- *"I found the fact that he presented on a real demo he had done made it very engaging and helpful to see how these topics are applied in the real world."*
- *"He had entertaining visuals and was able to bind his topic and seminar with applications people use daily."*

In Seminar 2 on Blockchain and Digital Forensics, participants valued the clarity of explanations and the use of practical examples that grounded the content in real-world applications:

- *"I was astonished with the Walmart example at the beginning taking 7 to 8 days and then working with IBM it got down to 2 seconds. Great way to prove the point."*
- *"I found it helpful that the speaker quickly explained the basics behind certain concepts before going into a more detailed explanation on her topic."*

In Seminar 3 on Post-Quantum Cryptography, participants were drawn to the timeliness and depth of the content, as well as the presenter's ability to make a complex topic understandable:

- *"I really liked this seminar, because she made a topic that is hard to understand actually make sense."*

- *"I really enjoyed the enthusiasm of the speaker and the focus on how the future of the industry is being shaped by quantum."*

In Seminar 4, the VICEROY Internship Scholar Panel resonated strongly with participants, who found their peer experiences both motivating and relevant to their professional development. Consistent with previous seminars, attendees also expressed a continued preference for sessions on career development topics:

- *"I loved having students around my age that have gone through the experiences. It was really cool to get insight about what projects they did and some interview prep."*
- *"This was great and is very applicable to where I am at as a student and a professional. Please do more industry and career focused ones in the future."*

Areas for Improvement

While participants' responses across the fall 2025 seminar series were mostly positive, open-ended feedback also highlighted areas for improvement for each seminar.

In Seminar 1 on Cyber-Physical System Recovery, the most consistent concern was pacing and information density. Participants noted that the seminar moved quickly through complex material and that certain graphs and visual representations were difficult to follow:

- *"I would like more information on the graphs and how those were developed."*
- *"I found it challenging keeping up with all the information being presented, especially with how quickly the seminar was paced."*

In Seminar 2 on Blockchain and Digital Forensics, participants similarly identified pacing and information density as the primary challenge, and others also noted that more foundational context at the outset would have strengthened their understanding:

- *"Some of the research is still kind of hard for me to understand. There are a lot of graphs, acronyms, letters, and numbers on the screen that don't connect well in my mind."*
- *"Present slower and possibly start the seminars by diving deeper into general concepts to help solidify the foundation of cybersecurity concepts."*

In Seminar 3 on Post-Quantum Cryptography, pacing of the presentation also emerged as a concern, with participants noting that slides were at times too dense and difficult to process:

- *"It was a lot of information shared very quickly, and it was hard to take notes with how fast the amount of information was shared."*
- *"The slides were very crowded and busy and it kind of was distracting and I would find myself reading it instead of listening fully to what was being said."*

During Seminar 4, the VICEROY Internship Scholar Panel, participants had few concerns, and one student expressed a desire for more details on specific internship experiences, such as information on securing mentorship. Another student also expressed a desire to ask questions rather than wait until the end of the panel presentations:

- *“They all brushed over getting a mentor. I would have liked to know more about that process.”*
- *“I think it is hard to save questions to the end at times since it is easy to forget in between the four presentations.”*

2026 SPRING SEMINAR SERIES

The 2026 spring seminar series consisted of six expert and scholar-led presentations addressing emerging topics in cybersecurity research, professional ethics, and student scholarship and capstone projects. The topics were as follows:

- Machine Learning to Evaluate Governance, Risk, and Compliance Associated with Large Language Model – Dr. Upakar Bhatta (Central Washington University) - February 3, 2026
- Securing Machine Learning: Evolving Threats, Attacks, and Defenses – Dr. Steve Wang (University of Idaho) - February 17, 2026
- Beyond the Harm Principle: What Students Can Teach Us About Cyber-Sanctity – Dr. Sherri Lynn Conklin (WSU) - March 3, 2026
- Scholarship Opportunities for Cybersecurity Students – Dr. Assefaw Gebremedhin (WSU) - March 24, 2026
- Cybersecurity Capstone Projects and Conferences - Student Panel - April 7, 2026
- Hardware IP Protection and Reliability Solutions in a Fully Transparent World – Dr. Leon Li (WSU) - April 21, 2026

Methods

Following each seminar, participants completed a survey via Qualtrics. The survey was similar to the questions used in the fall 2025 data collection. Across all six spring 2026 seminars, an average of 10 participants completed the survey (with session-level responses ranging from 5 to 18). Demographic data from survey respondents are presented below in Figures 9 and 10

Figure 9. Spring 2026 Participants' Gender

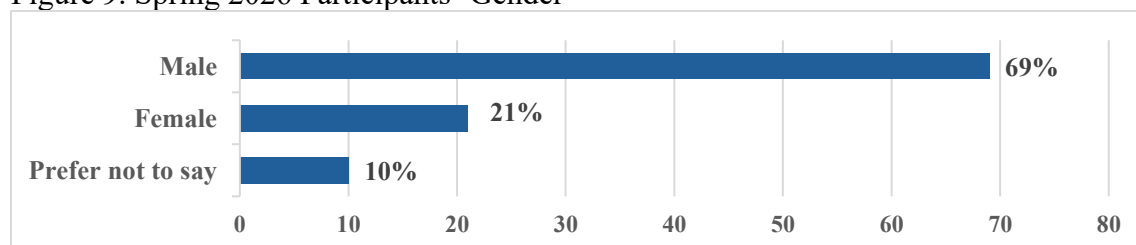
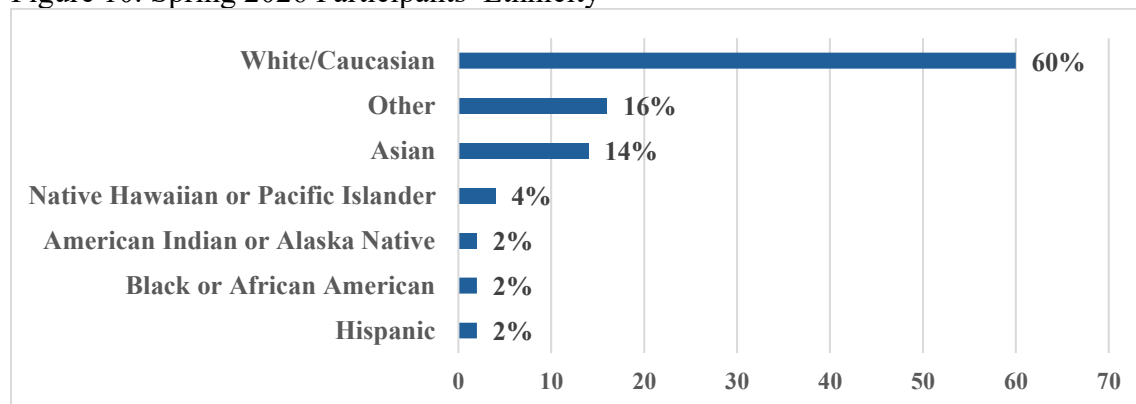


Figure 10. Spring 2026 Participants' Ethnicity



Key Findings

Perceived Satisfaction

Participants rated their overall satisfaction with the spring 2026 seminar series on a scale from *extremely dissatisfied* to *extremely satisfied*. Overall, 44% of participants rated themselves as extremely satisfied, 36% as somewhat satisfied, 16% as neutral, 2% as dissatisfied, and 2% as extremely dissatisfied (see Figure 11 for participants' overall perceived satisfaction with the spring 2026 seminar series). Satisfaction ratings for each seminar session offer a comprehensive understanding of participants' experiences across the spring 2026 seminar series, with the Securing Machine Learning session recording the highest level of extreme satisfaction among participants:

Seminar 1: Machine Learning to Evaluate Governance, Risk, and Compliance Associated with Large Language Models

- 33% rated being extremely satisfied
- 56% reported being somewhat satisfied
- 11% indicated a neutral level of satisfaction

Seminar 2: Securing Machine Learning: Evolving Threats, Attacks, and Defenses

- 61% rated being extremely satisfied
- 23% reported being somewhat satisfied
- 8% indicated a neutral level of satisfaction
- 8% reported being somewhat dissatisfied

Seminar 3: Beyond the Harm Principle: What Students Can Teach Us About Cyber-Sanctity

- 44% rated being extremely satisfied
- 44% reported being somewhat satisfied
- 12% indicated a neutral level of satisfaction

Seminar 4: Scholarship Opportunities for Cybersecurity Students

- 40% rated being extremely satisfied
- 40% reported being somewhat satisfied
- 20% indicated a neutral level of satisfaction

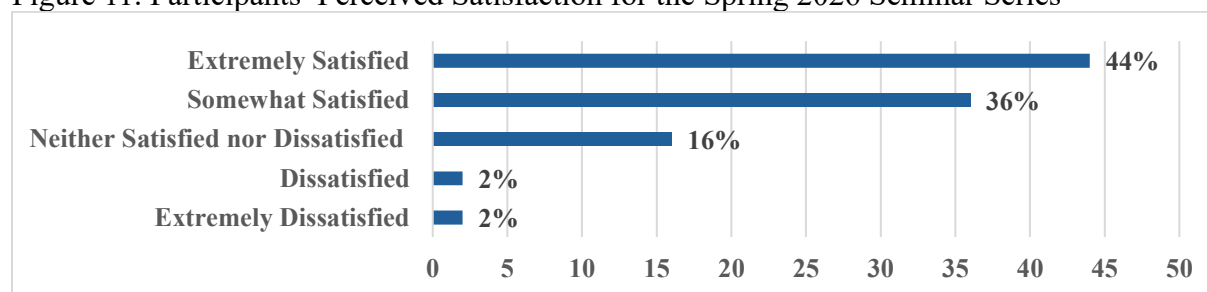
Seminar 5: Cybersecurity Capstone Projects and Conferences

- 36% rated being extremely satisfied
- 55% reported being somewhat satisfied
- 9% indicated a neutral level of satisfaction

Seminar 6: Hardware IP Protection and Reliability Solutions in a Fully Transparent World

- 50% rated being extremely satisfied
- 33% indicated a neutral level of satisfaction
- 17% rated being extremely dissatisfied

Figure 11. Participants' Perceived Satisfaction for the Spring 2026 Seminar Series



Perceived Effectiveness

Participants rated the effectiveness of each seminar in promoting their understanding of cybersecurity concepts on a scale from *very low* to *very high*. Overall, 51% rated effectiveness as very high, 33% as somewhat high, 13% as average, and 3% as somewhat low (see Figure 12 for participants' perceived effectiveness for the spring 2026 seminar series). Below is a breakdown of effectiveness ratings for each seminar session in the spring 2026 seminar series, with the Scholarship Opportunities session recording the highest level of very high effectiveness ratings among participants:

Seminar 1: Machine Learning to Evaluate Governance, Risk, and Compliance Associated with Large Language Models

- 39% rated effectiveness as very high
- 39% rated it as somewhat high
- 22% rated it as average

Seminar 2: Securing Machine Learning: Evolving Threats, Attacks, and Defenses

- 54% rated effectiveness as very high
- 23% rated it as somewhat high
- 15% rated it as average
- 8% rated it as somewhat low

Seminar 3: Beyond the Harm Principle: What Students Can Teach Us About Cyber-Sanctity

- 33% rated effectiveness as very high
- 22% rated it as somewhat high
- 33% rated it as average
- 12% rated it as somewhat low

Seminar 4: Scholarship Opportunities for Cybersecurity Students

- 80% rated effectiveness as very high
- 20% rated it as somewhat high

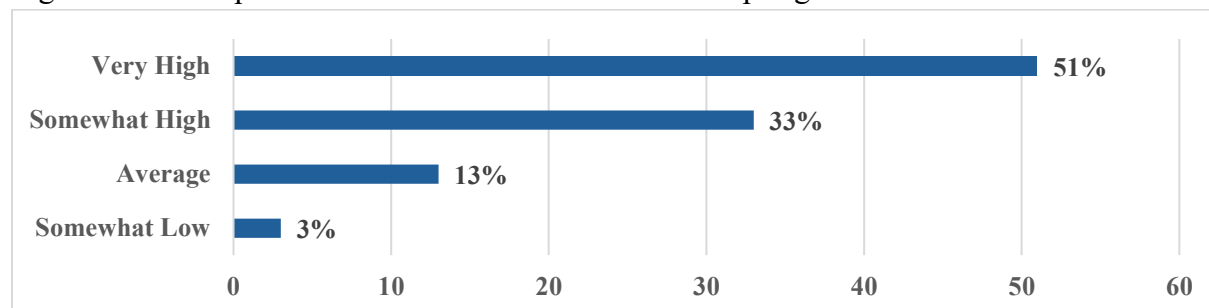
Seminar 5: Cybersecurity Capstone Projects and Conferences

- 46% rated effectiveness as very high
- 46% rated it as somewhat high
- 8% rated it as average

Seminar 6: Hardware IP Protection and Reliability Solutions in a Fully Transparent World

- 50% rated effectiveness as very high
- 50% rated it as somewhat high

Figure 12. Participants' Perceived Effectiveness for the Spring 2026 Seminar Series



Perceived Engagement

Participants rated the extent to which each seminar was engaging in supporting their learning of cybersecurity concepts on a scale from *strongly disagree* to *strongly agree*. Across the spring 2026 series, 43% of participants strongly agreed the seminars were engaging, 36% somewhat agreed, 20% neither agreed nor disagreed, and 1% somewhat disagreed (refer to Figure 13 for perceived engagement across the spring 2026 seminars). Each seminar's engagement rating provides additional insight into participant experiences, with the Hardware IP Protection session recording the highest level of strong agreement among participants:

Seminar 1: Machine Learning to Evaluate Governance, Risk, and Compliance Associated with Large Language Models

- 50% strongly agreed the seminar was engaging
- 33% somewhat agreed
- 17% neither agreed nor disagreed

Seminar 2: Securing Machine Learning: Evolving Threats, Attacks, and Defenses

- 53% strongly agreed the seminar was engaging
- 31% somewhat agreed
- 8% neither agreed nor disagreed
- 8% somewhat disagreed

Seminar 3: Beyond the Harm Principle: What Students Can Teach Us About Cyber-Sanctity

- 33% strongly agreed the seminar was engaging
- 11% somewhat agreed
- 56% neither agreed nor disagreed

Seminar 4: Scholarship Opportunities for Cybersecurity Students

- 20% strongly agreed the seminar was engaging
- 80% somewhat agreed

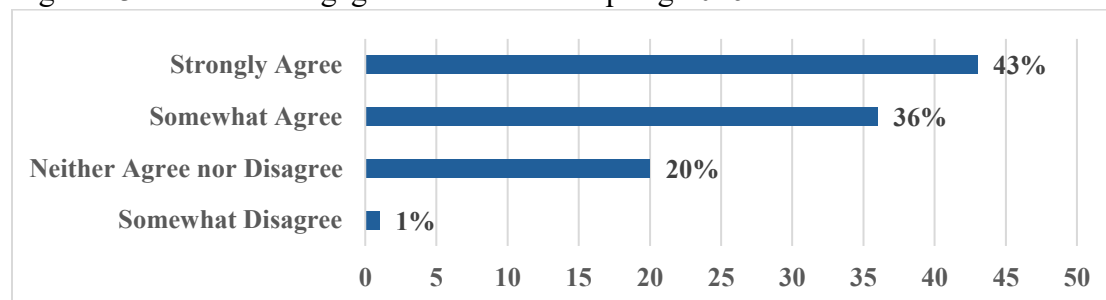
Seminar 5: Cybersecurity Capstone Projects and Conferences

- 36% strongly agreed the seminar was engaging
- 45% somewhat agreed
- 19% neither agreed nor disagreed

Seminar 6: Hardware IP Protection and Reliability Solutions in a Fully Transparent World

- 66% strongly agreed the seminar was engaging
- 17% somewhat agreed
- 17% neither agreed nor disagreed

Figure 13. Perceived Engagement across the Spring 2026 Seminars



Perceived Relevance

Participants rated the relevance of each seminar's content to their needs or interests on a scale from *not at all relevant* to *highly relevant*. Across the spring 2026 series, 38% of participants rated the content as highly relevant, 38% as relevant, 17% as somewhat relevant, and 7% as slightly relevant. No participants indicated the content was not at all relevant (see Figure 14 for participants' perceived relevance for the spring 2026 seminar series). Each seminar's relevance rating provides additional insight, with the Securing Machine Learning session recording the highest level of highly relevant ratings among participants:

Seminar 1: Machine Learning to Evaluate Governance, Risk, and Compliance Associated with Large Language Models

- 28% rated the content as highly relevant
- 44% rated it as relevant
- 28% rated it as somewhat relevant

Seminar 2: Securing Machine Learning: Evolving Threats, Attacks, and Defenses

- 62% rated the content as highly relevant
- 30% rated it as relevant
- 8% rated it as slightly relevant

Seminar 3: Beyond the Harm Principle: What Students Can Teach Us About Cyber-Sanctity

- 22% rated the content as highly relevant
- 22% rated it as relevant
- 45% rated it as somewhat relevant
- 11% rated it as slightly relevant

Seminar 4: Scholarship Opportunities for Cybersecurity Students

- 20% rated the content as highly relevant
- 60% rated it as relevant
- 20% rated it as slightly relevant

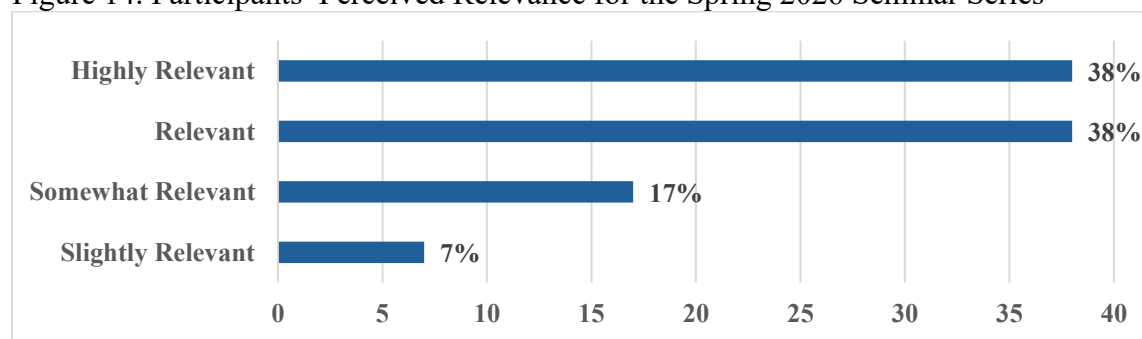
Seminar 5: Cybersecurity Capstone Projects and Conferences

- 46% rated the content as highly relevant
- 27% rated it as relevant
- 27% rated it as somewhat relevant

Seminar 6: Hardware IP Protection and Reliability Solutions in a Fully Transparent World

- 50% rated the content as highly relevant
- 50% rated it as relevant

Figure 14. Participants' Perceived Relevance for the Spring 2026 Seminar Series



Perceived Quality

Participants rated the overall quality of each seminar on a scale from *very poor* to *excellent*. Overall, 49% rated the quality as excellent, 33% as good, 17% as fair, and 1% as poor (see Figure 15 for participants' perceived seminar quality). A session-by-session examination of quality ratings provides additional insight into participant experiences across the spring 2026 seminar series, with the Securing Machine Learning session recording the highest level of excellent ratings among participants:

Seminar 1: Machine Learning to Evaluate Governance, Risk, and Compliance Associated with Large Language Models

- 33% rated the quality as excellent
- 39% rated it as good
- 22% rated it as fair
- 6% rated it as poor

Seminar 2: Securing Machine Learning: Evolving Threats, Attacks, and Defenses

- 69% rated the quality as excellent
- 23% rated it as good
- 8% rated it as fair

Seminar 3: Beyond the Harm Principle: What Students Can Teach Us About Cyber-Sanctity

- 33% rated the quality as excellent
- 11% rated it as good
- 56% rated it as fair

Seminar 4: Scholarship Opportunities for Cybersecurity Students

- 60% rated the quality as excellent
- 40% rated it as good

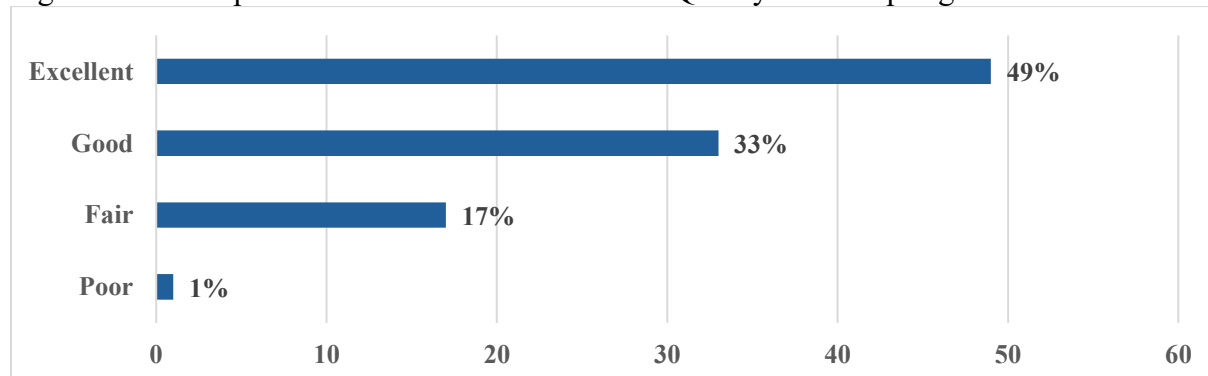
Seminar 5: Cybersecurity Capstone Projects and Conferences

- 46% rated the quality as excellent
- 54% rated it as good

Seminar 6: Hardware IP Protection and Reliability Solutions in a Fully Transparent World

- 50% rated the quality as excellent
- 33% rated it as good
- 17% rated it as fair

Figure 15. Participants' Perceived Seminar Overall Quality for the Spring 2026 Seminar Series



Positive Experiences

Participants' open-ended responses indicated high satisfaction, effectiveness, quality, relevance, and engagement ratings reported across the spring 2026 seminar series.

In Seminar 1 on Machine Learning and LLM Governance, participants valued the practical foundation of the content, particularly the use of diagrams and real-world examples that made complex governance frameworks more accessible. Several participants also appreciated the presenter's ability to connect the material to current cybersecurity challenges:

- *"The speaker provided good insight into the background and prerequisite knowledge. This helped set the information I needed to know for the seminar."*
- *"I found it helpful that he discussed how GRC applies to AI because that is more important now than ever."*

In Seminar 2 on Securing Machine Learning, participants highlighted the clarity of visual aids and the relevance of real-world examples, including demonstrations of graphs to understand the content of the presentation:

- *“I really enjoyed the taxonomy graphs the guest shared with us. It helped me see the structure of what is going on with attacks in machine learning.”*
- *“I found the real-world examples of how machine learning is used, like the Tesla example, with that example I liked how showing how small changes in something like images of stop signs can create enough confusion to be read as a 45 mph speed limit sign.”*

In Seminar 3 on Cyber-Sanctity, participants appreciated the novel framing of cybersecurity through an ethical lens, with several noting the value of connecting purity and sanctity principles to practical cybersecurity issues:

- *“The connection between the Purity/Sanctity foundation and real cybersecurity issues like phishing and third-party trackers was eye-opening.”*
- *“I liked hearing about how the ethical principles and cybersecurity principles align.”*

In Seminar 4 on Scholarship Opportunities, participants found the session useful for understanding available funding and program options. Participants valued the CyberCorps Scholarship for Service information and international opportunities:

- *“Understanding that CyberCorps and SFS were closely related was helpful.”*
- *“Learning about the overseas program.”*

In Seminar 5 on Capstone Projects and Conferences, participants appreciated hearing directly from peers about their experiences with cybersecurity competitions, conferences, and capstone expectations:

- *“I really liked hearing about the different experiences from the students, especially about how they prepare for cyber competitions and going to conferences.”*
- *“All the student-led seminars have been excellent. Seminars related to career and course opportunities are great.”*

In Seminar 6 on Hardware IP Protection, participants valued the visual presentation of complex hardware security concepts and the structured comparison of different defense mechanisms:

- *“I liked how there were different graphs and seeing the comparisons of different methods.”*
- *“I liked the description of randomization for adding opportunities to detect errors and the idea of considering scalability as a practical concern.”*

Areas for Improvement

Participants’ responses across the spring 2026 seminar series reflected positive experiences; however, the open-ended responses also identified areas for improvement.

In Seminar 1 on Machine Learning and LLM Governance, participants noted that the presentation was at times dense and unfocused, with slides that were difficult to read. They also suggested that to alleviate technical issues, presenters can send their slides ahead of the seminar:

- *“The seminar had a habit of meandering and being a bit unfocused at times, which made it more difficult to get a focused understanding of the material.”*
- *“Please request presenters to send their slides ahead of time, such that you can download and present them in case their machine cannot.”*

In Seminar 2 on Securing Machine Learning, participants again identified pacing and technical complexity as challenges, particularly around advanced concepts:

- *“There was a lot of information that was being taught very quickly. It was difficult to keep up.”*
- *“The topic was interesting but the talk itself was very technical. I would appreciate a little more explanation of the specifics.”*

In Seminar 3 on Cyber-Sanctity, participants noted that the session lacked sufficient practical cybersecurity content and that the presenter’s line of reasoning was at times difficult to follow:

- *“There wasn’t much practical knowledge of cybersecurity given.”*
- *“I had more difficulty following the speaker’s train of thought.”*

In Seminar 4 on Scholarship Opportunities, participants raised concerns about relevance for students in different academic stages. Participants would also appreciate other funding opportunities aside from SFS:

- *“For seniors, the information may be less applicable.”*
- *“Are there other funding ideas besides SFS?”*

In Seminar 5 on Capstone Projects and Conferences, a participant requested broader information for non-WSU participants and other consortium institutions. Another participant requested information for sessions on time management:

- *“Since I am not a student at WSU, the WSU cybersecurity capstone did not have much relevant information for me.”*
- *“It could be helpful to hear about time management to do a bunch of extra work and studying on their own.”*

In Seminar 6 on Hardware IP Protection, participants noted that the technical level of the content was challenging for those without a hardware background, suggesting that more foundational context at the outset would have improved comprehension:

- *“Pretty technical for my level.”*
- *“I think some of the aspects were a little complicated for our level of knowledge.”*

Recommendations for Future Seminars

Sustain and prioritize the hybrid seminar format that integrates career development content with research-based cybersecurity concepts. Participants across both semesters expressed a strong preference for this format. Program coordinators should continue to ensure that future seminar topics balance technical research content with practical career and professional development.

Encourage presenters to provide foundational context and scaffolding before advancing to complex technical material. Pacing and information density were the most consistently identified areas for improvement across both semesters. Participants with limited prior knowledge in a given topic area found it difficult to follow presentations that moved quickly through advanced content without first establishing key definitions and concepts.

Incorporate more interactive and applied components within seminar sessions. Participants across both semesters expressed a desire for greater interactivity, noting that opportunities to engage directly with content rather than passively receiving it would strengthen their learning experience.

Consider the diversity of participants' class levels and institutional affiliations when selecting and framing seminar topics. Feedback from both semesters indicated that certain sessions felt less relevant to participants due to their class level, field of study, or home institution. For example, scholarship and funding sessions were perceived as less applicable by seniors nearing graduation, capstone-related content was less relevant to non-WSU participants, and highly specialized technical sessions were more challenging for participants without a background in that specific area.

2026 CYBERSECURITY EDUCATION AND RESEARCH SUMMER WORKSHOP

The 2026 CySER Summer Workshop was held in person on the WSU Pullman campus from May 18 to May 22. The workshop provided sessions that integrated cybersecurity research and education with professional competencies, including teamwork, communication, leadership, and lifelong learning. It incorporated presentations, hands-on activities, panel discussions, and student poster presentations. Additionally, the workshop incorporated two field trips to Schweitzer Engineering Laboratories (SEL) in Pullman and Moscow.

Activity Implementations

Presentations

Across the five days of the workshop, participants attended a series of expert-led presentations spanning technical cybersecurity research, emerging technology, professional ethics, and career development. Presentations were delivered by faculty, researchers, and industry professionals from Washington State University, Montana State University, Syracuse University, and national defense organizations:

- Introductions and Cybersecurity at WSU - Partha Pande, Venera Arnaoudova & James Crabb, CySER
- DoD Speaker: Keynote Address - CJ Maciag
- Cybersecurity Scholarships at WSU - Assefaw Gebremedhin
- Post-Quantum Cryptography - Feng-Hao Liu,
- Hardware Security - Leon Li
- Formal Methods for Software Security - Kristopher Micinski (Syracuse)
- Behavioral Threats and Organizational Security - Rob Crossler
- Software Contracts for Secure Coding - Thomas Gilray
- Journalism, Security, and Digital Repression - Jennifer Henrichsen
- AI for Intrusion Detection Systems - James Halvorsen
- Cybersecurity in Advanced Manufacturing Systems - Satyajit Mojumder
- Improving Vulnerability Management - Ann Marie Reinhold (Montana State)
- Making the Most of Your Internships - Lisa Hathaway
- Lifelong Learning and Workshop Survey - Sola Adesope

Hands-on Activities

Three hands-on activities were integrated across the workshop to provide participants with experiential engagement with cybersecurity concepts. Each activity was facilitated by speakers with expertise in the respective topic area. The following hands-on activities took place during the workshop:

- Cyber Ethics - Sherri Lynn Conklin
- Web Security - Xu Lin
- Agentic AI and Security - Parteek Kumar

Field Trips

On Days 3 and 4 of the workshop, participants attended two field trips to Schweitzer Engineering Laboratories (SEL). SEL is a key CySER industry partner that provides exposure to real-world cybersecurity practices in professional industry settings. The trips featured a panel discussion with SEL cybersecurity professionals covering career paths and strategies for career success, followed by a guided tour of the manufacturing facilities. The following field trips took place during the workshop:

- Schweitzer Engineering Laboratories Power Grid Components Facility, Pullman, Washington
- Schweitzer Engineering Laboratories Printed Circuit Board Manufacturing Site, Moscow, Idaho

Industry Panel

On Day 4 of the workshop, four cybersecurity industry professionals joined the workshop remotely to participate in a panel discussion. Panelists answered student questions, discussed their career paths, described a typical day in their roles, and offered practical advice on entering and thriving in the cybersecurity field and building professional networks. The following professionals participated in the industry panel:

- Nathan Kipp, Schweitzer Engineering Laboratories
- Laurent Njilla, Air Force Research Laboratory
- Slater Weinstock, Amazon
- Kenneth Eversole, OpsCompanion

Student Panel

On Day 5 of the workshop, five CySER students participated in a student panel discussion. Panelists shared their experiences with internships, capstone projects, cyber competitions, and club activities, offering insights into their academic and professional journeys within the CySER program. The following students participated in the panel:

- Collin Bale, Cybersecurity
- Caitlyn Boyd, Computer Science
- Lauren Caruso, Management Information Systems
- Adam Caudle, Computer Science
- Sean Hodgson, Cybersecurity

Poster Session

On Day 1 of the workshop, VICEROY CySER students presented research completed after the academic year, mentored by graduate students and faculty advisors. The poster session gave participants the opportunity to showcase their scholarly work and engage with peers and faculty about their research findings. Following the poster session, certificates were awarded to participants in recognition of their accomplishments and participation in the program.

Methods

To evaluate the workshop's effectiveness, the external evaluation team administered a post-workshop survey via Qualtrics on the final day of the event. The survey comprised 17 items, including Likert-scale and open-ended questions on participant learning, activity effectiveness, overall satisfaction, key takeaway, areas for improvement and demographic information (see Appendix B for the survey instrument). Refer to Figures 16 and 17 for graphical representations of participants' gender and ethnicity.

Figure 16. 2026 CySER Summer Workshop Participants' Gender

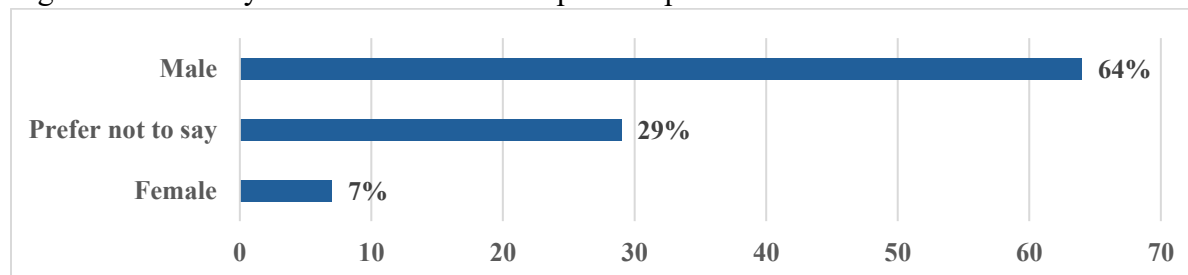
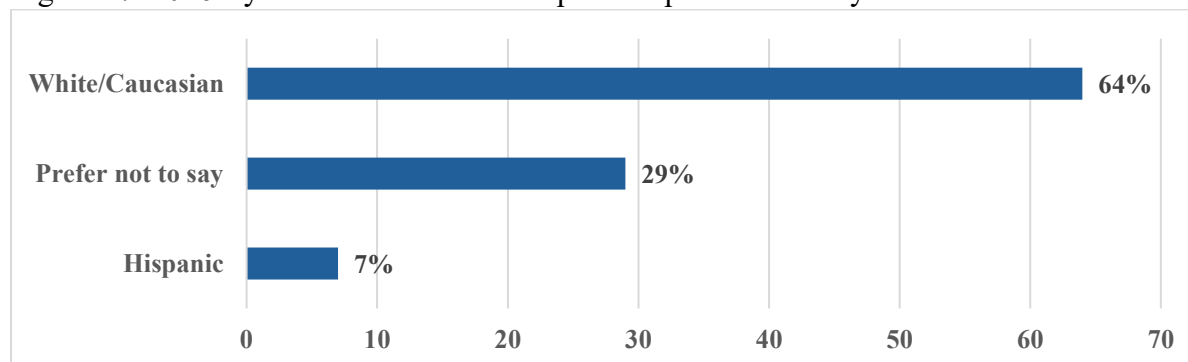


Figure 17. 2026 CySER Summer Workshop Participants' Ethnicity



Key Findings

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

Response to topics/hands-on during the workshop:

The first part of the post-workshop survey assessed participants' perceived learning across the various sessions and activities during the 2026 CySER Summer Workshop. Participants were asked to indicate the extent to which they learned from each topic, with responses ranging from *none at all* to *a great deal*. Refer to Tables 1, 2, and 3 for a breakdown of topics rated high, moderate, and low learning gains.

High-Rated Learning Topics ($\geq 70\%$)

A majority of participants (70% or more) reported that they learned *a lot* or *a great deal* from the following sessions, indicating the sessions' effectiveness in conveying cybersecurity concepts.

Table 1. High-Rated Topics

Topics	Percentage
Introductions and Cybersecurity at WSU	79%
Cybersecurity in Advanced Manufacturing Systems	79%
Hands-on Activity - Web Security	79%
Hands-on Activity - Agentic AI and Security	71%

Moderately Rated Topics (50 - 64%)

The following sessions received moderately strong learning ratings, with 50% to 64% of participants reporting that they learned *a lot* or a *great deal*.

Table 2. Moderately Rated Topics

Topics	Percentage
DoD Speaker: Keynote Address	64%
AI for Intrusion Detection Systems	64%
Improving Vulnerability Management	64%
Formal Methods for Software Security	57%
Cybersecurity Scholarships at WSU	50%
Post-quantum Cryptography	50%
Behavioral Threats and Organizational Security	50%
Journalism, Security, and Digital Repression	50%

Lower-Rated Topics (< 50%)

These sessions received relatively lower ratings, with fewer participants reporting significant learning gains.

Table 3. Lower Rated Topics

Topics	Percentage
Hardware Security	43%
Software Contracts for Secure Coding	43%
Lifelong Learning	43%
Hands-on Activity – Cyber Ethics	43%
Making the most of Your Internships	29%

These findings suggest that topics involving advanced theoretical or emerging technical content may require additional scaffolding to promote learning, especially for learners with limited prior exposure. The Web Security and Agentic AI activities were rated as highly impactful, with most participants reporting substantial learning gains.

Response to Activity Relating to Field Trips

Both field trips were well-received, with the Pullman visit earning particularly strong ratings. These findings reinforce the value of immersive, industry-based learning experiences in

contextualizing cybersecurity education for participants. See Table 4 for ratings reflecting participants' perceptions of how much they learned.

Table 4. Field Trips Ratings

Field Trips	Percentage
SEL Pullman	79%
SEL Moscow	64%

Response to Activity Relating to Poster Presentations and Panels

The industry panel and student poster presentations were highly valued components of the workshop. The student panel received moderate ratings, suggesting an opportunity to strengthen the format or preparation structure to increase perceived learning gains. Refer to Table 5 for ratings of how students perceived the poster presentations and panels.

Table 5. Poster Presentation and Panel Ratings

Topics	Percentage
Poster Presentations	71%
Industry Panel	64%
Student Panel	50%

Measuring the Effectiveness of the Workshop

Participants rated the overall effectiveness of each workshop component in promoting their cybersecurity learning using a scale from *very low* to *very high*. Results show that hands-on activities and field trips received the highest ratings during the 2026 CySER Summer Workshop, with nearly all participants rating them somewhat high or very high in effectiveness. The lower ratings for lectures emphasize the need for more interactive and practical learning experiences. These findings suggest expanding hands-on and field-based components, as these resonate strongly with participants. Refer to Table 6 for detailed ratings of each component as somewhat high or very high in effectiveness.

Table 6. Effectiveness of Workshop Components

Topics	Percentage
Hands-on Activities	93%
Field Trips	93%
Poster Presentation	71%
Industry Panel	57%
Student Panel	57%
Lectures	43%

Findings on Key Things Learned from the Workshop

To assess the workshop's alignment with participants' academic and professional goals, attendees were asked to respond to open-ended questions about their most important takeaways and how they intended to apply them in their career pursuits. The responses highlighted four consistent themes in participant learning. First, many participants noted that the workshop

broadened their understanding of the scope and interdisciplinary reach of cybersecurity, connecting it to artificial intelligence, hardware, manufacturing, and national defense:

- *“I got a great tour of the variety of topics cybersecurity plays a role in.”*
- *“The importance of hardware and software security and what agentic AI is and how it can be better integrated... Future of AI, bridging the gap of cybersecurity into industry.”*

Second, hands-on activities and field trips were identified as the most meaningful learning experiences. Participants with limited prior technical experience found the hands-on activities particularly valuable:

- *“I really found the hands-on learning valuable, especially with zero prior experience in coding. I got to learn pen testing, dabbled in some JavaScript, and learned how to set up an AI with n8n.”*
- *“The SEL tours were so enlightening on their practices and production.”*

Third, participants identified career development content, including the industry panel, student panel, and internship guidance sessions, as valuable in helping them formulate next steps toward career goals. Many participants noted that they left the workshop with a clearer sense of how to navigate their career pathways:

- *“I will apply what I have learned here to my internship this summer, as I have learned a great deal as to how to make the most out of it.”*
- *“I now have a clearer path on how to pursue my career and advance my knowledge.”*

Fourth, they valued the networking opportunities with professionals and peers. Many participants identified networking as among their most important takeaways from the week:

- *“Networking and connections are everything. That will be my biggest takeaway from this week.”*
- *“Built a lot of new connections with both speakers and other students.”*

Recommendations for Future Workshops

We commend the principal investigators and key personnel for their exemplary implementation of the 2026 CySER Summer Workshop. Notably, many of the previous year’s recommendations were 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 workshops, the following recommendations are offered based on the participants’ feedback:

Increase the number of hands-on activities integrated throughout the workshop. Hands-on activities were consistently rated as the most effective component of the workshop, and participants across multiple responses expressed a desire for more of these experiences.

Incorporating at least one hands-on activity per day, including optional after-hours sessions, would further strengthen knowledge retention.

Ensure presentations are accessible to participants across varying levels of technical background. A recurring theme in participant feedback was that some sessions moved too quickly through advanced technical content without sufficient foundational context. Presenters should be encouraged to define key technical terms before advancing to more complex concepts.

Retain and build upon the SEL field trip experience. The field trips to Schweitzer Engineering Laboratories were among the highest-rated components of the workshop, and student feedback expressed a desire to continue them.

Develop more structured and intentional networking opportunities for participants. Networking emerged as a valued outcome of the workshop. The addition of a networking event, such as a career fair or networking session would provide participants with more deliberate opportunities to build connections with industry professionals, peers, and faculty.

Consider incorporating a leadership development session into the workshop agenda. Participant feedback suggested interest in a session addressing leadership skills, particularly in the context of ROTC and national defense career pathways. Adding a leadership development component would complement the existing career preparation content and further align the workshop with CySER's mission of preparing scholars for the cybersecurity workforce.

Diversify the range of industry sectors represented in presentations and panel discussions. While the technical content of the workshop was well received, participants expressed interest in hearing from professionals across a broader range of industries, including healthcare, finance, and advanced manufacturing.

Conclusion

CySER continues to demonstrate strong progress toward its mission to prepare a skilled, diverse, and nationally engaged cybersecurity workforce. The 2025-2026 program year produced strong outcomes, including a first-place finish at the 2026 VICEROY Competition and high participant satisfaction and self-reported learning across the seminars and the summer workshop. The evaluation findings presented in this report provide a clear foundation for refining cybersecurity education and research programs in the coming year.

Appendix A: 2026 Fall/Spring Seminar Survey

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 most challenging and why?

Q7 The seminar was engaging in learning about cybersecurity concepts

- ☐ 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. Do you currently participate in the SFS program?

- ☐ Yes
- ☐ No

Q14 What is your current status or position at the school?

- ☐ Freshman
- ☐ Sophomore
- ☐ Junior
- ☐ Senior
- ☐ Graduate student
- ☐ Doctoral student
- ☐ Postdoctoral Fellow
- ☐ Faculty
- ☐ Staff
- ☐ Other

Q15 What is your gender?

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

Q16 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: 2026 CySER Summer Workshop Survey

Thank you for participating in the 2026 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 15 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 To what extent did each of the following presentations enhance your understanding of the topic?

	None at all	A little	A moderate amount	A lot	A great deal
Introductions and Cybersecurity at WSU	☐	☐	☐	☐	☐
DoD Speaker: Keynote Address	☐	☐	☐	☐	☐
Cybersecurity and Scholarships at WSU	☐	☐	☐	☐	☐
Post-Quantum Cryptography	☐	☐	☐	☐	☐
Hardware Security	☐	☐	☐	☐	☐
Formal Methods for Software Security	☐	☐	☐	☐	☐

Q2 To what extent did each of the following presentations enhance your understanding of the topic?

	None at all	A little	A moderate amount	A lot	A great deal
Behavioral Threats and Organizational Security	☐	☐	☐	☐	☐
Software Contracts for Secure Coding	☐	☐	☐	☐	☐
Journalism, Security, And Digital Repression	☐	☐	☐	☐	☐
AI for Intrusion Detection Systems	☐	☐	☐	☐	☐
Cybersecurity in Advanced Manufacturing Systems	☐	☐	☐	☐	☐

Q3 To what extent did each of the following presentations enhance your understanding of the topic?

	None at all	A little	A moderate amount	A lot	A great deal
Improving Vulnerability Management	☐	☐	☐	☐	☐
Making the Most of your Internships	☐	☐	☐	☐	☐
Lifelong Learning	☐	☐	☐	☐	☐

Q4 To what extent did each of the hands-on activities enhance your understanding of cybersecurity concepts?

	None at all	A little	A moderate amount	A lot	A great deal
Hands-on Activity – Cyber Ethics	☐	☐	☐	☐	☐
Hands-on Activity – Web Security	☐	☐	☐	☐	☐
Hands-on Activity – Agentic AI and Security	☐	☐	☐	☐	☐

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 student 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 Overall, how would you rate the effectiveness of the following components in promoting your learning about cybersecurity?

	Very High	Somewhat High	Average	Somewhat Low	Very Low
Lectures	☐	☐	☐	☐	☐
Poster Presentations	☐	☐	☐	☐	☐
Hands on Activities	☐	☐	☐	☐	☐
Field Trips	☐	☐	☐	☐	☐
Industry Panel	☐	☐	☐	☐	☐
Student Panel	☐	☐	☐	☐	☐

Q10 Please indicate the degree to which you agree with these statements

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
The workshop activities were engaging	☐	☐	☐	☐	☐
I was satisfied with the variety of topics presented at the workshop	☐	☐	☐	☐	☐
The workshop was relevant to my career goals	☐	☐	☐	☐	☐
The workshop increased my interest in pursuing a career in cybersecurity	☐	☐	☐	☐	☐
I built meaningful connections with peers during the workshop	☐	☐	☐	☐	☐
There were sufficient networking opportunities	☐	☐	☐	☐	☐
The annual workshop was well organized	☐	☐	☐	☐	☐

Q11 What are three most important things you learned from this workshop?

Q12 How will you apply what you learned from this workshop to your career pursuits?

Q13 Please share your suggestions for how future workshops could be improved.

Q14 Please enter your program level.

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

Q15 What is your gender Identity

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

Q16 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 (please identify)
- ☐ Prefer not to say

Q17 Please provide the name of your university or institution
