

The Report of the

2023 NSF Cybersecurity Summit for

Large Facilities and Cyberinfrastructure

October 23-26, 2023

Hosted as an in-person and virtual conference

<https://www.trustedci.org/2023-cybersecurity-summit>

Acknowledgements

The Summit would not have been possible without the commitment and dedicated work of many individuals. The organizers wish to thank all those who attended this year’s Summit. Special gratitude goes to all who responded to the call for participation (CFP), spoke, provided training, and actively participated, including the 2023 Program Committee (highlighted in [*Section*](https://docs.google.com/document/d/1Su-PaDi-OBkUO_kibAE1SYhp23Hej4XDb54q8Ey28xk/edit#heading=h.qd7a5qo76ado) *4*), without whom the event would not have been as successful. Our sincere thanks goes to the National Science Foundation (NSF) and Indiana University’s Center for Applied Cybersecurity Research (CACR) for making this community event possible.

This event was supported by the NSF under award number 2241313. Any opinions, findings, and conclusions or recommendations expressed at the event or in this report are those of the authors and do not necessarily reflect the views of the NSF.

About this Report

This document is the product of Trusted CI, The NSF Cybersecurity Center of Excellence, and was supported by the NSF under award number 2241313.

Citing this Report

Please cite as: Julie Songer and John Zage. Report of the 2023 NSF Cybersecurity Summit for Cyberinfrastructure and Large Facilities. DOI: 10.5281/zenodo.10372658

License

This work is made available under a Creative Commons Attribution-ShareAlike 4.0 International license (<https://creativecommons.org/licenses/by-sa/4.0/>).

For the latest information on the Summit, please see: <https://www.trustedci.org/2023-cybersecurity-summit>

### 

[**Executive Summary**](#_heading=h.1fob9te) **[4](#_heading=h.1fob9te)**

[**1 Plenary Sessions**](#_heading=h.3znysh7) **5**

[1.1 Presentations](#_heading=h.2et92p0) **5**

[1.2 Panels](#_heading=h.23ckvvd) **8**

[**2 Realtime Training and Workshop**](#_heading=h.1t3h5sf)**s 9**

**3** [**Common Themes and Challenges**](#_heading=h.4d34og8) **12**

**4** [**Summit Management and Planning**](#_heading=h.2s8eyo1) **12**

**5** [**Summit Attendee Demographics**](#_heading=h.17dp8vu) **13**

**6** [**Summary of Summit Survey Responses**](#_heading=h.35nkun2) **14**

**7** [**Conclusion**](#_heading=h.1ksv4uv) **14**

[**Appendix A: Summit Agenda**](#_heading=h.ihv636) **16**

[**Appendix B: Speakers and Trainers**](#_heading=h.32hioqz) **19**

[**Appendix C: Student Participation**](#_heading=h.1hmsyys) **22**

[**Appendix D: NSF Project Representation**](#_heading=h.41mghml) **22**

[**Appendix E: Attendee Survey Report**](#_heading=h.3o7alnk) **25**

# 

# Executive Summary

The *2023 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure* continued a decade-long tradition of providing a forum for National Science Foundation (NSF) scientists, researchers, cybersecurity, and cyberinfrastructure (CI) professionals and stakeholders to develop community and share best practices.

Trusted CI, NSF’s Cybersecurity Center of Excellence, has hosted the annual event since 2013.

The 2023 Summit was held in person in Berkeley, CA, at the Lawrence Berkeley National Laboratory, October 23-26. A virtual attendance option was available. Please see *Appendix A* for the full *Summit Agenda*.

AI’s impact on cybersecurity, managing cybersecurity risks, and Trusted CI Framework adoption were important themes at the Summit. Please see *Section 3 Common Themes and Challenges.*

The number of individuals who registered for the 2023 Summit was 321, including nine students, and 12 of 17 NSF Major Facilities. Attendees represented 44 NSF projects. Attendees enjoyed the in-person collaboration opportunities but continued to recognize the advantages of the virtual format.

The Summit had representation from four countries, the same as the 2022 Summit. The number of student attendees increased from 17 in 2022 to 22 this year. Please see *Appendix C* for information about the 2023 Summit student attendees.

Relevant content and relationship-building events resulted in an engaging and productive 2023 Summit. In a follow-up survey 100 percent of attendees rated their overall experience with the 2023 Summit as Excellent or Good.

The Trusted CI team looks forward to the 2024 Summit, taking place October 7-10 at Carnegie Mellon University in Pittsburgh, PA, so we can continue to advance the mission of the NSF science community.

# 1 Plenary Sessions[[1]](#footnote-1)

## 1.1 Presentations

Slides provided by the presenters can be found [here](https://docs.google.com/document/d/e/2PACX-1vS12c-mQLAWgND0sBDfCj_Vyj2j9C73Wx8RMF479DwlUTOGQAYI3IFRKXPaHdv2Ced6HP2WreJQ03L7/pub).

Day 2 Plenary sessions

**NSF Welcome** *– Robert Beverly*

Robert Beverly, NSF program officer with the Office of Advanced Cyberinfrastructure (OAC), discussed exciting developments at the OAC and its mission to enable scientific discovery through an integrated, accessible, and robust cyberinfrastructure ecosystem.

Among many initiatives, the OAC is spearheading a National AI Research Resource (NAIRR) task force to strengthen and democratize the U.S. AI innovation ecosystem in a way that protects privacy, civil rights, and civil liberties. NAIRR goals are to spur innovation, increase diversity of AI talent, improve U.S. capacity for AI research and development, and advance trustworthy AI.

Beverly emphasized that changes in users, technology, vendors, and the national landscape require us to think deeply about our collective AI strategy for the future.

**Cybersecurity at Major Facilities: Current Directions and Issues: New Issues, Old Problems** *– Michael Corn*

Michael Corn, cybersecurity advisor for Research Infrastructure at the NSF, emphasized the importance of facility resilience. With the sophistication of modern, state-sponsored or facilitated attacks, breaches of accounts and systems are inevitable. To counter the ongoing threat, he focused on three themes:

* Cybersecurity is risk management
* A cybersecurity program requires leadership engagement
* An effective program builds resilience

NSF major facilities are considered critical infrastructure in the U.S. National competitiveness and reputation are at risk even without loss of data. As a result, Corn said there is increased pressure on the NSF to become more prescriptive regarding cybersecurity requirements. He predicts more demanding requirements within the next five years.

**Berkeley & ESNet Welcome** – *Sean Peisert and Adam Slagell*

Sean Peisert, senior scientist of Computing Sciences Research, Berkeley Lab, and deputy director and co-PI of Trusted CI, welcomed Summit attendees to the Berkeley Lab. He discussed the origins of the Berkeley Lab and its mission of bringing science solutions to the world. And he described the Computing Sciences Research mission of achieving transformational impacts in science through the discovery and use of advanced computational methods, making them accessible to the broad science community.

Adam Slagell, chief information security officer, introduced ESnet and SAFER. The Energy Sciences Network (ESnet) is a high-performance, unclassified network built to support scientific research. Funded by the Department of Energy (DOE) Office of Science and managed by Lawrence Berkeley National Laboratory, ESnet provides services to more than 50 DOE research sites, including the entire National Laboratory system, its supercomputing facilities, and its major scientific instruments. ESnet also connects to 140 research and commercial networks, permitting DOE-funded scientists to collaborate productively with global partners. Slagell also introduced Security Assistance for Education and Research (SAFER), an international security trust group focused on protecting research and education. Esnet and Berkeley Lab are founding members of SAFER.

**Trusted CI Update** *–* *Jim Basney*

Jim Basney, director of Trusted CI, welcomed attendees and thanked all those who made the Summit possible, including Berkeley Lab staff and presenters. Basney encouraged attendees to stay connected to monthly webinars, and to make plans to attend the 2024 Summit, October 7-10, at Carnegie Mellon University in Pittsburgh, PA.

**Keynote: Social Engineering Manifestations as Ransomware Attacks Unfold** *– Dr. Aunshul Rege*

Dr. Aunshul Rege is the director of Cybersecurity in Application, Research, and Education Lab at Temple University and was a Trusted CI Fellow in the 2019 inaugural year. He introduced the ransomware social engineering intrusion chain of reconnaissance, point of entry, ransom note, negotiation, followed by customer support or punishment.

His reconnaissance example was the attack on MGM Resorts. The attacker found an employee on LinkedIn, then called the help desk. The $34 billion company was defeated by a 10-minute conversation. Phishing, he said, is the most common form used for point of entry. Ransom notes, he said, rely on authority, scarcity/urgency, and reciprocity. For negotiation, psychological and open-source intelligence persuasion is used by the attackers. Customer support needs business savvy and brand reputation. Punishment results in reputational damage.

While hacking is often successful due to mistakes people make, Dr. Rege believes training can make a difference in preventing hacking.

**Implementing NIST 800-171 in a decentralized and centralized environment** – *Laura Elkin*

The University of Cincinnati (UC) is helping faculty research initiatives with the Department of Defense (DoD):

1. UC set up a steering committee to guide university leaders in adopting NIST 800-171 in centralized and decentralized environments.
2. To properly implement the NIST 800-171 framework in a mixed environment requires creativity and collaboration.
3. The effort helps researchers doing DoD research with Controlled Unclassified Information clauses.

**Unmasking Shadows: Investigating MICI-BICA, an Incident Involving IRC-Based Malware Deployment, Rootkit Stealth, and Self-Hiding Cryptominers** –*Pau Cutrina Vilalta, Romain Wartel*

European security researchers investigated a cybercrime group’s exploitation of university networks using an Internet Relay Chat network, rootkits for stealth, and self-hiding malware to execute cryptominers:

1. The investigation uncovered attack vectors, methods of infiltration, and deployment of malicious tools.
2. The research detailed steps taken to identify and mitigate the threat and measures employed to enhance the security posture of affected institutions.
3. The researchers are sharing their results with the research and education sector, empowering other organizations to defend against similar threats.

**Black Hole Locker Ransomware: Affiliate program** – *Romain Wartel and Pau Cutrina*

The Black Hole Locker affiliate program was created by former security experts.

1. The security researchers are based between the French and Swiss border.
2. Tech professionals are invited to be affiliates in the program.

Day 3 Plenary sessions

**Principles of Decentralized Cyberinfrastructure** *– John Haverlack*

In Alaska, there are many extremes and critical CI services need to be locally hosted and independent of Internet access.

1. Cut cables and geomagnetic storms are two examples of loss of CI in Alaska. How to provide food, medical, and financial services without CI?
2. Decentralized CI is needed to recover from wide-scale disaster events and avoids single points of dependency.
3. Access to LDC CI must be open to everyone, should be free of gatekeepers, and should be cross cultural and multilingual.

Day 4 Plenary sessions

**U.S. Academic Research Fleet (ARF) Cyber Risk Management Program (CRMP)** *– Mikeal Jones*

This presentation reviewed the International Maritime Organization cybersecurity requirements and the delegation of cyber risk management responsibilities to ship operators in the U.S.

1. The ARF security team at OmniSOC has developed a successful CRMP.
2. The CRMP provides an achievable and effective framework to meet IMO compliance.

**Cyber Forensics in Everyday Business** *– Chris Lauderbaugh*

Cyber and data forensics are valuable tools for law enforcement when investigating potential criminal activity.

1. Forensic tools and methods can be used in everyday cybersecurity operations to build more robust response playbooks, understand attacker actions, and inform defense.
2. Whether it is data recovery, incident response, or securing critical systems, putting forensic measures in place early can help protect research cyberinfrastructure from attack and data loss.

## 1.2 Panels

**Inclusion, Diversity, Equity, and Accountability**

**Moderator:** *Kevin Nichols*

**Panelists:** *James Masteller, Soledad Antelada Toledano, Cheryl Washington, Damian Rouson*

The goal of a panel discussion on Inclusion, Diversity, Equity and Accountability (IDEA) was to provide an environment psychologically safe for an open/candid discussion. The panel focused on four primary questions as well as supporting participation from attendees:

1. The word "trusted" is used repeatedly throughout the marketing materials for this conference. How do you build "trust" with individuals from different backgrounds and experiences?

2. NSF's Diversity Initiatives Mission stated on its website, is "To recruit, retain and develop a diverse, high-performing workforce that draws from all segments of society and values fairness, diversity, and inclusion to promote the progress of science." Why do you think that this is important? How challenging is it to accomplish this mission?

3. NSF's Strategic Goal 2: Under Workplace Inclusion, seeks to "Cultivate a culture that encourages collaboration, flexibility, and fairness to enable individuals to contribute to their full potential and further retention." How can Trusted CI create a culture like this? What are some barriers that it needs to overcome?

4. What do you think the members of this audience can do starting today to help NSF achieve its diversity initiatives?

**Experiences from SIO (CCVR), OSU (RCRVs), OOI, and USAP in Cybersecure-by-Design Maritime and Polar Design and Construction**

**Moderator:** *Sean Peisert*

**Panelists:** *Chris Romsos, Jon Meyer, Ezra Van Everbroeck, Craig Risien, Tim Howard*

The panel discussed Trusted CI’s recent “secure by design” efforts with institutions responsible for design and procurement of vessels that will join the NSF’s U.S. Academic Research Fleet, as well as institutions procuring underwater vehicles.

1. Oregon State University is taking delivery of NSF Research Class Research Vessels (RCRV). Trusted CI supported cybersecurity aspects of the RCRV acceptance testing process and the security-focused design and procurement requirements for the CCRV.
2. Scripps Institution of Oceanography is designing the California Coastal Research Vessel (CCRV).
3. Ocean Observatories Initiative is refreshing its glider and underwater autonomous vehicle fleet.
4. The U.S. Antarctic Program is supporting Trusted CI’s research in maritime and polar operational technology given their experiences in designing the Antarctic Research Vessel and planned refreshes of the three U.S. Antarctic facilities.

**Trusted CI Fellows Panel**

**Moderator:** *Rick Wagner*

**Panelists:** *Andrew Ferbert, David White, Lori Sussman, Nick Harrison, Ramazan Aygun, Gary Rogers, Phuong Cao*

2023 Trusted CI Fellows gave brief presentations on what they learned about cybersecurity in the context of their respective disciplines. Key points about the Trusted CI Fellows program:

1. Empowers members of the scientific community with basic knowledge of cybersecurity. They serve as cybersecurity liaisons to their respective community.
2. Fosters professional development in cybersecurity by providing access to training and other resources to a network of diverse Fellows.
3. Fellows champion cybersecurity in their scientific and geographic communities and communicate challenges and successful practices to Trusted CI.

# 2 Realtime Training and Workshops

Day 1 Workshops

**Zeek Training: Hands on Zeep Scripting** – *Aashish Sharma*

Attendees learned the fundamentals of Zeek scripting along with some practical exercises.

**Zeek Training: Intermediate to Zeek**– *Fatema Bannat Wala, Christian Kreibich, Keith Lehigh*

Attendees were trained how to run a real-world Zeek installation on their own hardware.

**Jupyter Security Workshop** – *Rick Wagner*

Attendees learned about the role of security in the Jupyter community in providing users, developers, and system administrators with trustworthy software, processes, and documentation for scientific computing.

**WISE Community Workshop**– *David Kelsey and Romain Wartel*

The workshop facilitated discussions on Security for Collaborating Infrastructures and how to collaborate with the Trusted CI Framework.

Day 2 Workshops

**Securing your Code with Better Coding Practices and Tools** – *Bart Miller and Elisa Heymann*

Attendees learned skills critical for software developers and security analysts with a focus on web programming practices that can avoid security vulnerabilities.

**Jupyter Network Monitoring with Zeek Workshop** *– Rick Wagner, Christian Kreibich, Fatema Bannat Wala*

The workshop focused on how network monitoring with Zeek can safeguard Jupyter deployments.

**Security Intrusion at the Zebra Scientific Alliance** *– Romain Wartel*

The gamified security incident response exercise put 20 to 25 participants to the test in collaborating and solving an attack.

Day 3 Workshops

**Deep Machine Learning for Intrusion Detection in Cyber-Physical Critical Infrastructures** *– Muhammad Ismail*

The workshop covered best practices for developing practical testbeds of cyber-physical critical infrastructures with an example of electric power systems and provided a hands-on approach for developing deep machine learning techniques for intrusion detection.

**Physical Security is Important Um’k** *– Adrian Crenshaw, Susan Sons*

Discussion of physical security flaws and how intruders get around them. It’s important to know your environment and monitor it. Policies and procedures must be in place and spread throughout the culture.

**Regulatory Compliance for Research: DFARS/CMMC, HIPAA, GDPR, NSPM-33** *– Anurag Shankar, Will Drake, Tim Daniel, Scott Russell*

Attendees were introduced to current and upcoming rules and regulations that affect research and strategies to tackle them.

**Catch Me if you GPT: Tutorial on Deepfake Texts** *– Adaku Uchendu, Thai Le, Dongwon Lee*

The training delivered a comprehensive tutorial of recent literature on the detection and obfuscation of deepfake text authorships. Hands-on examples and quizzes generated interactive participation.

**The Trusted CI Framework: Strategies for Getting Started** *– Scott Russell, Craig Jackson*

The training explored strategies for adopting the Framework, setting effective priorities and timelines, and overcoming obstacles.

**BOF: Research Security Compliance Collaborations to Support PI-Research***– Laura Elkin, Lauren Schroeder, Maria Bunch*

The University of Cincinnati and Texas A&M shared processes that were helpful in reducing the burden on research principal investigators (PIs). The discussion generated ideas for PIs and their support teams to take back to their institutions.

**BoF: NICE Workforce Framework Adoption: Cybersecurity Teaching Innovations** *– Lori Sussman*

Discussion on the University of Southern Maine’s Cybersecurity Ambassador Program that provides opportunities for students to use cybersecurity knowledge and skills to raise cyber safety awareness in the community.

Day 4 Workshops

**How We Failed to Handle a Triple-Combo Attack Against the R&E HPC Community Worldwide…In the Middle of a Pandemic** *– Romain Wartell*

The workshop focused on mistakes and lessons learned during global attacks on the R&E HPC community during the pandemic. Explicit and pragmatic recommendations were shared on how to handle such large-scale intrusions more effectively in the future.

**Monero Mining, with Love, From Space** *– Romain Wartell*

The workshop covered how malicious attacks on the International Space Station were detected, how the malicious activity was traced back to a privileged insider, and the following administrative and technical challenges that followed.

**Security Log Analysis** *– Mark Krenz, Ishan Abhinit*

The workshop walked participants through the security log analysis lifecycle, providing considerations for centralized log collection and log management tools, phases of compromise, and examples from real attacks.

**pDNSSOC: Correlating DNS logs with Threat Intel from MISP as a Poor Man’s SOC** *– Romain Wartell, Pau Cutrina Vilalta, Christos Arvantitis*

In the R&E sector, defending as a global community is a crucial strategy. This involves producing and sharing relevant threat intelligence across the entire sector. pDNSSOC provides a turn-key solution to both detect and respond to security incidents.

# 3 Common Themes and Challenges

The benefits and threats of AI to cybersecurity, managing cybersecurity risks, and Trusted CI Framework adoption were common themes during the Summit. The annual Summit serves as a supportive and collaborative community for NSF-affiliated researchers, cybersecurity professionals, and educators. When the community comes together for the Summit, they collectively learn from each other. The Summit offers practical solutions and helpful discussions for meeting challenges common to the higher education cybersecurity environment. Common themes during the 2023 Summit included:

* How AI can help and hurt cybersecurity measures
* How to manage cybersecurity and ransomware risks
* How to adopt the Trusted CI Framework
* How to build cybersecurity into design and procurement
* How to improve identity and access management
* How to address compliance challenges

# 4 Summit Management and Planning

The 2023 Summit was organized and hosted by Trusted CI, the NSF Cybersecurity Center of Excellence. Diana Cimmer, project management specialist, provided overall leadership for organizing the Summit. The Organizing Committee included Jim Basney, Leslee Bohland, Jeannette Dopheide, Sean Peisert, Jason Salinas, and Kelli Shute.

A Program Committee (PC) comprised key leaders from NSF CI projects and the broader community. The PC was charged with five core tasks for 2023: (a) setting Summit goals and establishing a Summit theme; (b) setting the specific agenda and inviting speakers; (c) selecting white papers and training for presentation at the Summit; (d) extending invitations to expert presenters; and (e) laying the framework for successful post-Summit evaluation and community support. Jim Marsteller served as chair of the PC, a role he held in prior Summits. The PC held 11 meetings by Zoom beginning March 24, 2023 and ending July 14, 2023. It conferred electronically prior to and following this time period.

The 2023 PC members were:

* **James Marsteller (Chair) -** Trusted CI
* **Fatema Bannat Wala -** security engineer, ESnet
* **Damian Clarke -** vice president, Technology Services, Alabama State University
* **Chris Morrison** - head of Information Technology Operations, NSF’s NOIRLab
* **Anita Nikolich** - director of Research and Technology Innovation and research scientist, University of Illinois Urbana-Champaign
* **Sean Peisert** - senior scientist, Lawrence Berkeley National Laboratory
* **Victor Piotrowski** - lead program director, National Science Foundation
* **Rick Wagner** - chief technology officer, University of California San Diego

The PC’s 2023 CFPmaintained the ongoing Summit mission to provide a format for increasing the NSF community’s understanding of cybersecurity strategies that strengthen trustworthy science: what data, processes, and systems are crucial to the scientific mission, what risks they face, and how to protect them. As in prior years, the CFP requested brief white papers that focused on NSF Major Facilities’ unmet cybersecurity challenges, lessons learned, and/or significant successes. Training and workshop proposals were requested with suggested topics of cybersecurity planning and programs, risk assessment and management, regulatory compliance, identity and access management, data management and provenance, network security and monitoring, secure coding and software assurance, physical security in the context of information security, and information security of scientific and emerging technologies. Please see *Appendix A* for the Summit agenda.

# 5 Summit Attendee Demographics

The count of individuals who registered for the 2023 Summit was 321 including 22 students, 13 from the local university and nine who attended on scholarships. The Summit was open to all interested individuals with connections to the NSF-sponsored research, cybersecurity, and/or CI communities and NSF officials.

The Summit had representation from four countries, same as the 2022 Summit. The number of student attendees decreased from 17 in 2022 to nine this year. Please see *Appendix C* for information about the 2023 Summit student attendees.

The NSF Cybersecurity Summit aims to foster and provide a welcoming environment of mutual respect for all people. The organizers recognize that diverse participation is both a socially relevant outcome for NSF and a particular challenge in the cybersecurity community in general. To gather ongoing baseline data related to this diversity effort, attendees had the option to provide their ethnicity/race and gender/sex. The aggregated voluntary responses to those items follow in Tables 1 and 2.

**Table 1. Attendee self-reported ethnicity.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ethnicity/Race** | **2023** | **2022** | **2021** | **2020** | **2019** | **2018** |
| White or Caucasian | 91 (28.4%) | 126 (56.3%) | 191 (58.0%) | 141 (49.5%) | 88 (57.9%) | 84 (71.2%) |
| Asian or Southeast Asian | 26 (8.1%) | 32 (14.3%) | 41 (12.5%) | 28 (9.8%) | 16 (10.5%) | 8 (6.8%) |
| Prefer not to answer | 19 (5.9%) | 10 (4.5%) | 17 (5.2%) | 15 (5.2%) | 6 (3.9%) | 7 (5.9%) |
| Hispanic or Latino | 8 (2.5%) | 12 (5.4%) | 14 (4.3%) | 15 (5.2%) | 7 (4.6%) | 1 (0.8%) |
| Black or African American | 14 (4.4%) | 6 (2.7%) | 8 (2.4%) | 16 (5.6%) | 6 (3.9%) | 1 (0.8%) |
| Multiracial | 0 (0%) | 2 (0.9%) | 6 (1.8%) | 5 (1.8%) | 3 (2.0%) | 2 (1.7%) |
| Other Ethnicity | 3 (0.9%) | 2 (0.9%) | 1 (0.3%) | 1 (0.4%) | 0 (0%) | 1 (0.8%) |
| Middle Eastern | 0 (0%) | 0 (0%) | 1 (0.3%) | 1 (0.4%) | 0 (0%) | 0 (0%) |
| No Answer Provided | 160 (49.8%) | 34 (15.2%) | 50 (15.2%) | 63 (22.1%) | 26 (17.1%) | 14 (11.9%) |

**Table 2. Attendee self-reported gender.³**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Gender / Sex** | **2023** | **2022** | **2021** | **2020** | **2019** | **2018** |
| Female | 41 (12.8%) | 44 (19.6%) | 68 (20.7%) | 36(35.2%) | 27 (17.8%) | 18 (15.3%) |
| Male | 115 (35.8%) | 138 (61.6%) | 201 (61.1%) | 68(66.7%) | 96 (63.2%) | 75 (63.6%) |
| No Answer Provided | 154 (48.0%) | 32 (14.3%) | 57 (17.3%) | N/A[[2]](#footnote-2) | 28 (18.4%) | 25 (21.2%) |
| Non-Binary | 2 (0.6%) | 0 (0.0%) | 3 (0.9%) | 1(1.0%) | 1 (0.7%) | 0 (0%) |
| Gender Non-Conforming | 0 (0%) | 1 (0.0%) |  |  |  |  |
| Prefer not to answer | 9 (2.8%) | 9 (4.0%) |  |  |  |  |

## 

# 6 Summary of Summit Survey Responses

In an effort to learn from each year’s Summit and to improve the following year’s experience, we solicited attendee feedback via a Google forms-based survey. The survey asked attendees about their overall Summit experience. We received 55 responses to the Summit Attendee Survey.

Of 55 respondents, 55 rated their overall experience with the 2023 Summit as Good or Excellent. A large majority, 44 of 55, said they would like to attend future Summits in person, 3 of 40 said remote, 8 were undecided. Of the 55 attendees who responded to the question, “How useful to your work was the information discussed at the Summit?” all found it to be Very, Moderately, or Extremely useful.

As in previous years, some attendees found the workshops were useful or important.

Additional attendee survey response detail can be found in *Appendix E*.

# 7 Conclusion

The dedication, creativity, and flexibility of the *2023 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure* planning committees and the Summit attendees resulted in a collaborative, enjoyable, and productive meeting. Survey responses from 54 of 55 attendees rated their overall experience with the 2023 Summit as Excellent or Good. Summit participants valued content addressing current issues, such as AI impact on cybersecurity, managing cybersecurity risks, and Trusted CI Framework adoption. The Trusted CI team looks forward to serving the NSF science community during the 2024 Summit to be held October 7-10 at Carnegie Mellon University in Pittsburth, PA.

Appendix A: Summit Agenda

****

**PROGRAM AGENDA**

2023 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure

**Program Committee Members**:

Jim Marsteller (chair), Fatema Bannat Wala, Damian Clarke, Chris Morrison, Anita Nikolich, Sean Peisert, Victor Piotrowski, Rick Wagner

**Organizers**:

Diana Cimmer (lead), Leslee Bohland, Jim Marsteller, Jeannette Dopheide, Sean Peisert, Jason Salinas, Kelli Shute, Jim Basney

*All Times Listed in Pacific Standard Time (PST)*

### **DAY 1 TRAINING DAY**

### Monday, October 23, 2023 (In-person only)

|  |  |
| --- | --- |
| **Time** | **Session title** |
| 9:00 am – 1:00 pm  1:00 pm – 2:00 pm | **Zeek Training: Hands on Zeek Scripting**  *Organizers: Aashish Sharma* |
| 9:00 am – 1:00 pm  1:00 pm – 2:00 pm | **Zeek Training: Intermediate to Zeek**  *Instructors: Fatema Bannat Wala, Christian Kreibich, Keith Lehigh* |
| 9:00 am – 1:00 pm  1:00 pm – 2:00 pm | **Jupyter Security Workshop**  *Instructors: Rick Wagner* |
| 1:00 pm – 2:00 pm | **WISE Community Workshop**  *Instructors: David Kelsey, Romain Wartel* |

### **DAY 2 PLENARY AND WORKSHOPS**

### Tuesday, October 24, 2023

Slides provided by the presenters can be found [here](https://docs.google.com/document/d/e/2PACX-1vS12c-mQLAWgND0sBDfCj_Vyj2j9C73Wx8RMF479DwlUTOGQAYI3IFRKXPaHdv2Ced6HP2WreJQ03L7/pub).

|  |  |
| --- | --- |
| **Time** | **Session title** |
| 7:00 am | **Sign-in and Continental Breakfast** |
| 8:00 am | **Update from the NSF Office of Advanced Cyberinfrastructure** (*Rob Beverly)* |
| 8:25 am | **Cybersecurity at Major Facilities: Current Directions and Issues** (*Michael Corn*) |
| 8:50 am | **Berkeley & ESnet Welcome** *(Sean Peisert and Adam Slagell)* |
| 9:05 am | **Trusted CI Update** (*Jim Basney*) |
| 9:30 am | **Keynote: Social Engineering Manifestations as Ransomware Attacks Unfold** *(Dr. Aunshul Rege)* |
| 10:30 am | **Refreshment Break** |
| 11:00 am | **Plenary Session: Implementing NIST 800-171 in a both decentralized and centralized environment** *(Laura Elkin)* |
| 11:30 am | **Plenary Session: Unmasking Shadows - Investigating MICI-BICA, an Incident Involving IRC-Based Malware Deployment, Rootkit Stealth, and Self-hiding Cryptominers** (*Pau Cutrina Vilalta, Romain Wartel)* |
| 12:00 pm | **Plenary Session: Black Hole Locker Ransomware - Affiliate Program** (*Romain Wartel, Pau Cutrina)* |
| 12:30 - 2:00 pm | **Lunch** |
| 2:00 - 5:00 pm | **Securing your Code with Better Coding Practices and Tools** *(Bart Miller, Elisa Heymann)* |
| 2:00 - 5:00 pm | **Jupyter Network Monitoring with Zeek Workshop** (*Rick Wagner, Christian Kreibich, Fatema Bannat Wala*) |
| 2:00 - 5:00 pm | **Security Intrusion at the Zebra Scientific Alliance** *(Romain Wartell)* |
| 5:30 – 7:30 pm | **Social Night** |

**DAY 3 PLENARY AND WORKSHOPS**

### Wednesday, October 25, 2023

|  |  |
| --- | --- |
| **Time** | **Session title** |
| 7:00 am | **Sign-in and Continental Breakfast** |
| 8:00 am | **Plenary Session: Principles of Decentralized Cyberinfrastructure** (*John Haverlack)* |
| 8:30 - 9:30 am | **Plenary Session: Inclusion, Diversity, Equity and Accountability (IDEA)*****Panel moderator*** *(Scott Russell)* |
| 9:30 am - 12:30 pm | **Deep Machine Learning for Intrusion Detection in Cyber-Physical Critical Infrastructures** *(Muhammad Ismail)* |
| 9:30 am - 12:30 pm | **Physical Security is Important Um’k** (*Adrian Crenshaw, Susan Sons*) |
| 9:30 am - 12:30 pm | **Regulatory Compliance for Research: DFARS/CMMC, HIPAA, GDPR, NSPM-33** *(Anurag Shankar, Will Drake, Tim Daniel, Scott Russell)* |
| 9:30 am - 12:30 pm | **SAFER Member Meeting (Members Only)** |
| 12:30 pm - 2:00 pm | **Lunch** |
| 2:00 pm | **Catch Me If You GPT: Tutorial on Deepfake Texts** *(Adaku Uchendu, Thai Le, Dongwon Lee)* |
| 2:00 pm | **BOF: Research Security Compliance Collaborations to Support PI Research** (*Laura Elkin, Lauren Schroeder, Maria Bunch)* |
| 2:00 pm | **The Trusted CI Framework Strategies for Getting Started** *(Scott Russell, Craig Jackson)* |
| 2:00 pm | **ACCESS CONNECT Cybersecurity Group and Invited Guests** *(Derek Simmel)* |
| 3:30 pm | **Refreshment Break** |
| 4:00 pm | **Catch Me If You GPT: Tutorial on Deepfake Texts** *(Adaku Uchendu, Thai Le, Dongwon Lee)* |
| 4:00 pm | **BOF: Research Security Compliance Collaborations to Support PI Research** (*Laura Elkin, Lauren Schroeder, Maria Bunch)* |
| 4:00 pm | **The Trusted CI Framework Strategies for Getting Started** *(Scott Russell, Craig Jackson)* |
| 4:00 pm | **SAFER Member Meeting Continued (Members Only)** |
| 5:00 pm | **Conclude** |

**DAY 4 PLENARY AND WORKSHOPS**

|  |  |
| --- | --- |
| **Time** | **Session title** |
| 7:00 am | **Sign-in and Continental Breakfast** |
| 8:00 - 11:00 am | **Trusted CI Framework Community of Practice (CoP) Quarterly Meeting (Members Only)** *(Ranson Ricks)* |
| 8:00 - 11:00 am | **Security Log Analysis** *(Mark Krenz, Ishan Abhinit, Phuong Cao)* |
| 8:30 am | **How We Failed to Handle a Triple-combo Attack Against the R&E HPC Community Worldwide…In the Middle of a pandemic** *(Romain Wartel)* |
| 9:00 am | **Monero Mining, With Love, From Space** *(Romain Wartel)* |
| 9:30 am | **Reserved: Open Floor for Attendees to Share TLP-Related Information** |
| 10:00 am | **Reserved: Open Floor for Attendees to Share TLP-Related Information** |
| 10:30 am - 12:00 pm | **pDNSSOC: Correlating DNS Logs with Threat Intel from MISP as a Poor Man’s SOC** *(Romain Wartel, Pau Cutrina Vilalta, Christos Arvantitis)* |
| 11:00 am - 12:00 pm | **Panel Session: Experiences from SIO (CCRV), OSU (RCRVs), OOI, and USAP in Cybersecure-by-Design Maritime and Polar Design and Construction** *(Sean Peisert)* |
| 12:00 - 1:30 pm | **Lunch** |
| 1:30 pm | **Plenary Session: U.S. Academic Research Fleet (ARF) Cyber Risk Management Program (CRMP)** *(Mikeal Jones)* |
| 2:00 pm | **Plenary Session: Cyber Forensics in Everyday Business** *(Chris Lauderbaugh)* |
| 2:30 pm | **Poster Session / Ice Cream Break / Refreshments** |
| 3:30 pm | **Plenary Session: Trusted CI Fellows Panel** *(Rick Wagner)* |
| 4:00 pm | **Plenary Session: Conference Round-up** |
| 4:30 pm | **Summit Observations and Feedback** |
| 5:00 pm | **Adjourn** |

# Appendix B: Speakers and Trainers

|  |  |  |
| --- | --- | --- |
| **Name** | **Institution** | **Job Title** |
| Ishan Abhinit | Indiana University, Center for Applied Cybersecurity Research | Senior Security Analyst |
| Christos Arvantitis | CERN | Computer Security Team Fellow |
| Ramazan Aygun | Kennesaw State University | Director, Center for Research Computing |
| Fatema Bannat Wala | ESnet | Security Engineer |
| Jim Basney | National Center for Supercomputing Applications, Trusted CI | Director, Trusted CI |
| Robert Beverly | NSF Office of Advanced Cyberinfrastructure | Program Officer |
| Maria Bunch | Texas A&M, Research Security Office | Compliance Officer |
| Phuong Cao | National Center for Supercomputing Applications | Research Scientist |
| Michael Corn | NSF | Cybersecurity Advisor for Research Infrastructure |
| Adrian Crenshaw | Indiana University, OmniSOC | Senior Security Analyst |
| Pau Cutrina Vilalta | CERN | Security Team |
| Tim Daniel | Indiana University, Center for Applied Cybersecurity Research | Information Security Analyst |
| Jeannette Dopheide | National Center for Supercomputing Applications, University of Illinois, Trusted CI | Senior Education, Outreach, and Training Coordinator |
| Will Drake | Indiana University, Center for Applied Cybersecurity Research | Chief Information Security Officer |
| Laura Elkin | University of Cincinnati | Cybersecurity Specialist |
| Andrew Ferbert | University of California San Diego | Platform Services Manager |
| Nick Harrison | North Carolina Community College | Information Security Officer |
| John Haverlack | University of Alaska | Cybersecurity Manager |
| Elisa Heymann | University of Wisconsin-Madison | Senior Scientist |
| Tim Howard | National Science Foundation Office of Polar Programs | Information Technology Support Manager and the Information Security Manager |
| Muhammad Ismail | Tennessee Tech University | Assistant Professor of Computer Science |
| Craig Jackson | Indiana University, Center for Applied Cybersecurity Research | Deputy Director |
| Mikeal Jones | Indiana University, OmniSOC | Security Analyst |
| Christian Kreibich | Corelight | Technical Lead (Open Source) |
| Mark Krenz | Indiana University, Center for Applied Cybersecurity Research | Chief Security Analyst |
| Chris Lauderbaugh | Indiana University, OmniSOC | Security Analyst |
| Thai Le | University of Mississippi | Assistant Professor |
| Dongwon Lee | Pennsylvania State University | Professor |
| Keith Lehigh | Indiana University | University Information Security Office |
| Jon Meyer | Scripps Institution of Oceanography, CCRV project | Information Systems Manager |
| Barton Miller | University of Wisconsin-Madison | Professor |
| Sean Peisert | Lawrence Berkeley National Laboratory | Senior Scientist |
| Aunshul Rege | Temple University, Cybersecurity in Application, Research and Education Lab | Director |
| Craig Risien | Oregon State University, OOI project | Project Manager |
| Ranson Ricks | Indiana University, Center for Applied Cybersecurity Research | Senior Project Manager |
| Gary Rogers | University of Tennessee | HPC Systems Administrator |
| Chris Romsos | Oregon State University, RCRV project | Systems Engineer |
| Scott Russell | Indiana University, Center for Applied Cybersecurity Research | Senior Policy Analyst |
| Laura Schroeder | Texas A&M Export Control Office | Director |
| Anurag Shankar | Indiana University, Center for Applied Cybersecurity Research | Senior Security Analyst |
| Aashish Sharma | Lawrence Berkeley National Laboratory | Cybersecurity Team |
| Derek Simmel | Pittsburgh Supercomputing Center | Senior Information Security Officer |
| Adam Slagel | ESnet | Chief Information Security Officer |
| Susan Sons | Indiana University, OmniSOC and Research SOC | Executive Director |
| Lori Sussman | University of Southern Maine | Assistant Professor of Technology and Cybersecurity |
| Adaku Uchendu | MIT Lincoln Lab | Information Security Officer |
| Ezra Van Everbroeck | Scripps Institution of Oceanography, CCRV project | Director of Information Systems |
| Rick Wagner | University of California San Diego | Chief Technology Officer |
| Romain Wartel | CERN | Security Officer |
| David White | Clemson University | Research Professor |

# Appendix C: Student Participation

Twenty-two students joined the Summit for four days of hands-on training, talks, panels, and active Q&A sessions. Below is a list of the students who agreed to share their names in the report.

|  |  |
| --- | --- |
| **Name** | **Institution** |
| Chad Calligari | University of South Alabama |
| Matheu Fletcher | University of Illinois at Urbana-Champaign |
| Robert Johnson | The University of Tennessee at Chattanooga |
| Kaneesha Moore | Mississippi State University |
| Kennedy Moore | Clark Atlanta University |
| Ololade Odunsi | University of New Haven |
| Henry Schmidt | University of Arkansas |
| Nathalia Soares | Louisiana State University |
| Aman Thanvi | University of Maryland, College Park |
| Ashmita Kumar | University of California, Berkeley |
| Oliver Lin | University of California, Berkeley |
| Hailey Pham | University of California, Berkeley |
| Adrian Segura | University of California, Berkeley |
| Ben Sikes | University of California, Berkeley |
| Helena Su | University of California, Berkeley |
| Owen Thompson | University of California, Berkeley |
| Alyssa Umino | University of California, Berkeley |
| Kiriratanak Vong | University of California, Berkeley |
| Rae Xin | University of California, Berkeley |
| Alice Yeh | University of California, Berkeley |

# 

# Appendix D: NSF Project Representation

The NSF projects represented at this year’s Summit were:

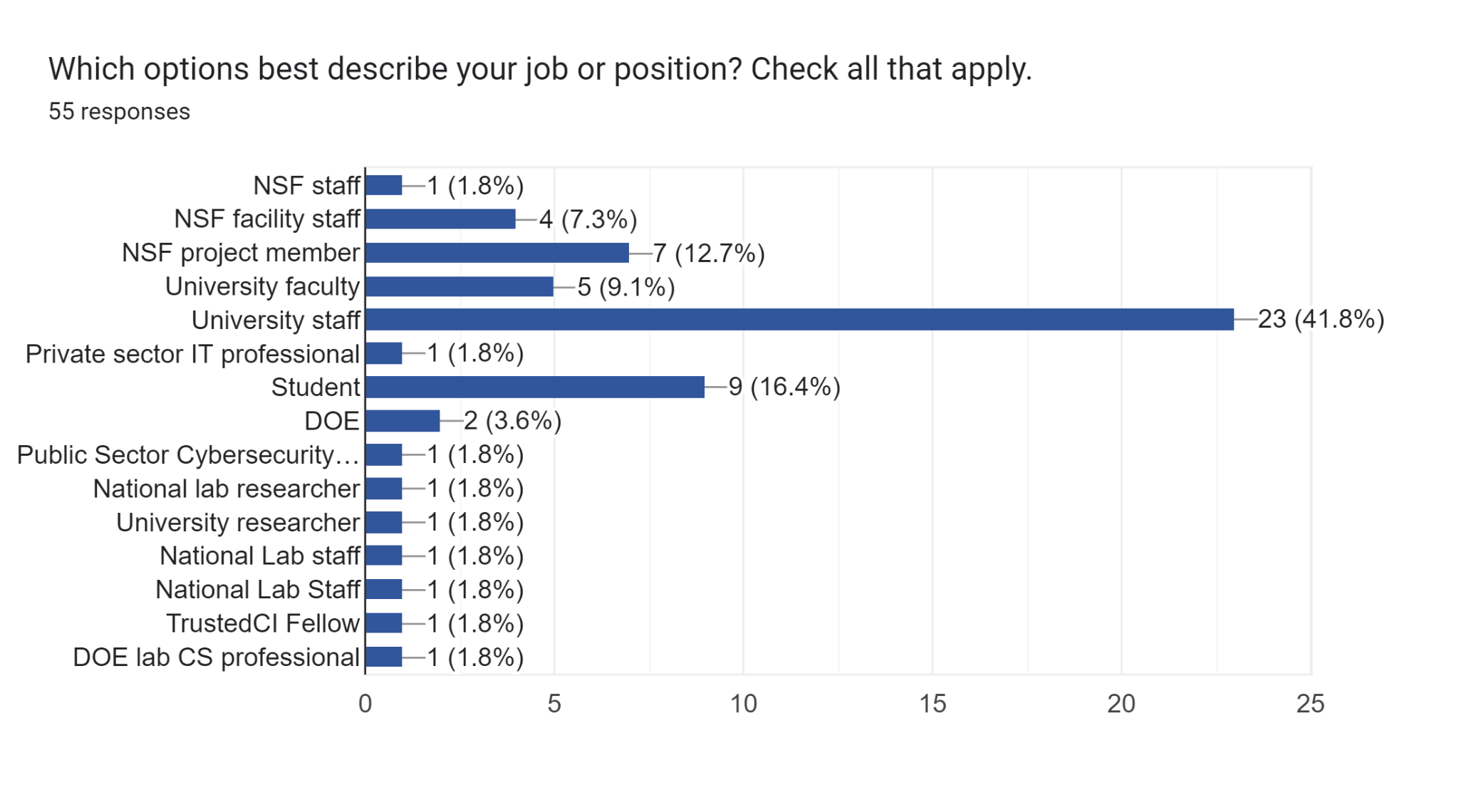
* ACO: An Open CI Ecosystem to Advance Scientific Discovery (OpenCI)
* Category I: Bridges-2: Scalable Converged Computing, Data, and Analytics for Rapidly Evolving Science and Engineering Research
* CC\* CIRA: Shared Arkansas Research Plan for Community Cyber Infrastructure (SHARP CCI)
* CC\* Data Storage: High Volume Data Storage Infrastructure for Scientific Research and Education at Kennesaw State University Shared as Open Science Data Federation Data Origin
* CCRI: Planning-C: A Community Research Infrastructure for Integrated AI-Enabled Malware and Network Data Analytics
* Center for Trustworthy Scientific Cyberinfrastructure
* Characterization of Chemosensory Pathways in Cnidarians
* CI CoE: CI Compass: An NSF Cyberinfrastructure (CI) Center of Excellence for Navigating the Major Facilities Data Lifecycle
* CICI: Center of Excellence: Center for Trustworthy Scientific Cyberinfrastructure
* CICI: Regional: Substrate for Cybersecurity Education; a Platform for Training, Research and Experimentation (SCEPTRE)
* CICI: UCSS: Building a Community of Practice for Supporting Regulated Research
* Collaborative Research: CCRI: NEW: Open Community Platform for Sharing Vehicle Telematics Data for Research and Innovation
* Collaborative Research: EAGER SaTC-EDU: Artificial Intelligence and Cybersecurity: From Research to the Classroom
* CyberCorps Scholarship for Service (Renewal): Cybersecurity meets Artificial Intelligence for preparing the Next Generation of Cybersecurity Professionals
* CyberTraining: Pilot: Interdisciplinary Cybersecurity Education to Support Critical Energy and Chemical Infrastructure
* FMitF: Track II: Bringing Verification-Aware Languages and Federated Authentication to Enable Secure Computing for Scientific Communities
* Frameworks: Software NSCI-Open OnDemand 2.0: Advancing Accessibility and Scalability for Computational Science through Leveraged Software Cyberinfrastructure
* HiSeasNet: Expanding Coverage and Real-Time Data Collection Capabilities for UNOLS Vessels
* I-Corps: Liveness detection and integrity authentication of digital audio
* LIGO Laboratory Operations and Maintenance 2019-2023
* Management and Operations of the Gemini Observatory
* Mid-scale RI-2 Consortium: Biogeochemical-Argo: A global robotic network to observe changing ocean chemistry and biology
* Mid-scale RI-2 Consortium: Network for Advanced NMR
* MRI: Acquisition of Autonomous Plug-In Hybrid Vehicle Platform for Multidisciplinary Research and Education at the University of Michigan-Dearborn
* National Radio Astronomy Observatory: Very Large Array Operations and Maintenance
* Natural Hazards Engineering Research Infrastructure: Computational Modeling and Simulation Center 2021-2025
* Natural Hazards Engineering Research Infrastructure: Experimental Facility with Large, Mobile Dynamic Shakers for Field Testing 2021-2025
* Natural Hazards Engineering Research Infrastructure: Natural Hazard and Disaster Reconnaissance (RAPID) Facility 2021-2025
* NSF's National Optical-Infrared Astronomy Research Laboratory (NOIRLab): Management and Operations of Vera C. Rubin Observatory
* Research Infrastructure: CC\* Data Storage: Rice Collaborative Object Store
* Research Infrastructure: Mid-scale RI-1 (M1:IP): SPHERE - Security and Privacy Heterogeneous Environment for Reproducible Experimentation
* SaTC-CCRI: Collaborative Research: Sharing Expertise and Artifacts for Reuse through Cybersecurity CommunityHub (SEARCCH) (SRI International)
* SaTC: CORE: Small: Linking2Source: Security of In-Vehicle Networks via Source Identification
* Ship-based Science Technical Support in the Arctic (STARC)
* Southern Ocean Carbon and Climate Observations and Modeling (SOCCOM2)
* Track 1: ACCESS Resource Allocations Marketplace and Platform Services (RAMPS)
* Track 2: Customized Multi-tier Assistance, Training, and Computational Help (MATCH) for End User ACCESS to CI
* Track 3: COre National Ecosystem for CyberinfrasTructure (CONECT)
* Track 4: Advanced CI Coordination Ecosystem: Monitoring and Measurement Services
* University of Alaska Fairbanks/Sikuliaq Oceanographic Instrumentation (2019)
* University of Alaska Fairbanks/Sikuliaq Oceanographic Instrumentation (2020)
* Virginia Tech CyberScholars Program

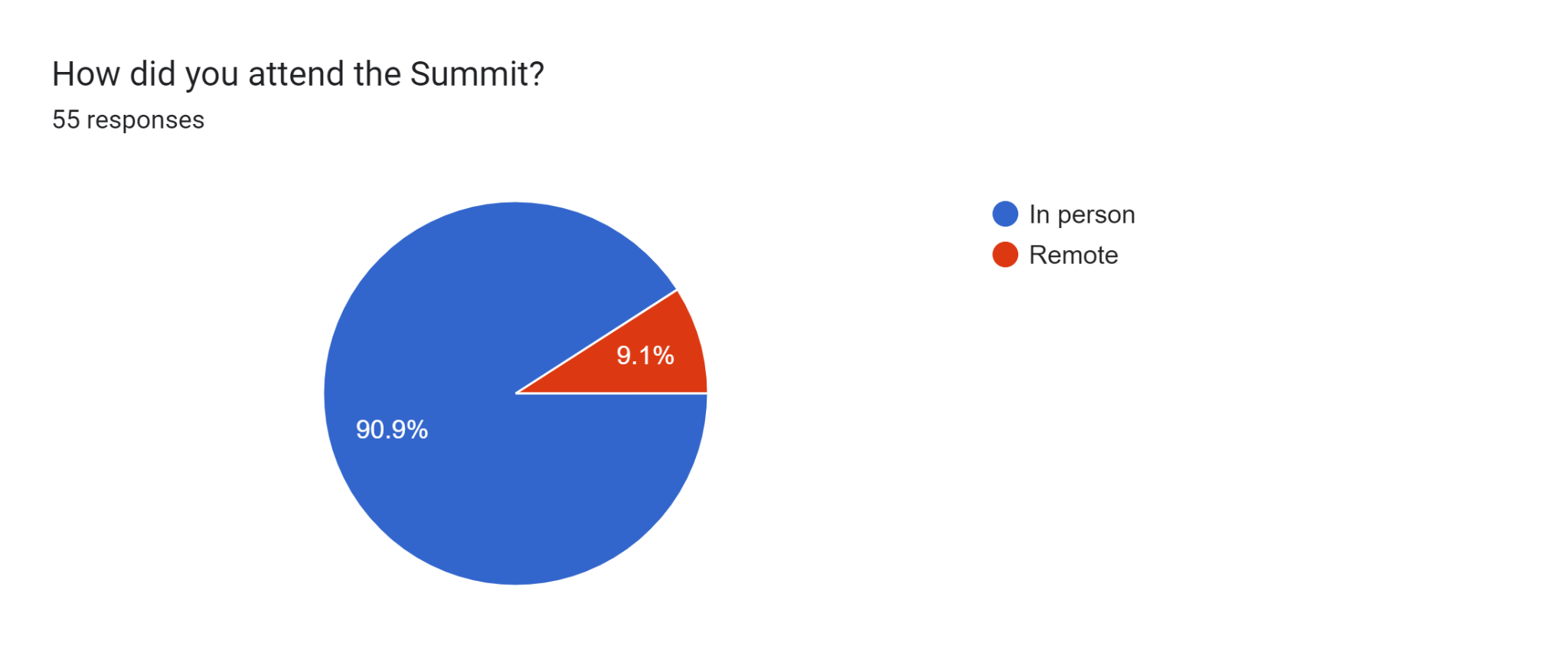
The 12 NSF Large Facilities represented at this year’s Summit were:

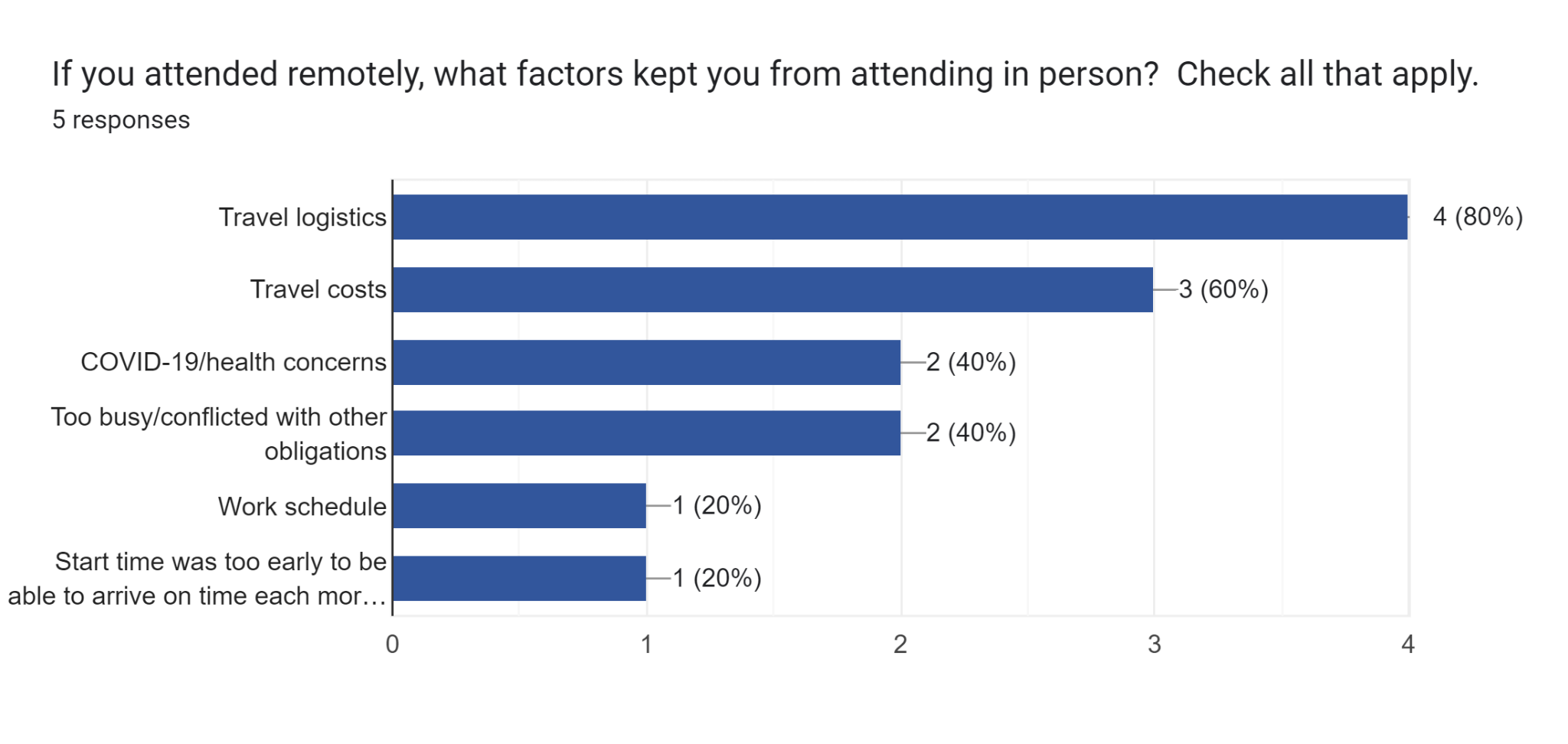
* Academic Research Fleet
* Icecube Neutrino Observatory
* International Ocean Discovery Program
* Green Bank Observatory
* Laser Interferometer Gravitational-wave Observatory
* National Center for Atmospheric Research
* National High Magnetic Field Laboratory
* National Radio Astronomy Observatory
* National Solar Observatory, Daniel K Inouye Solar Telescope
* NSF's National Optical-Infrared Astronomy Research Laboratory
* Ocean Observatories Initiative
* United States Antarctic Program

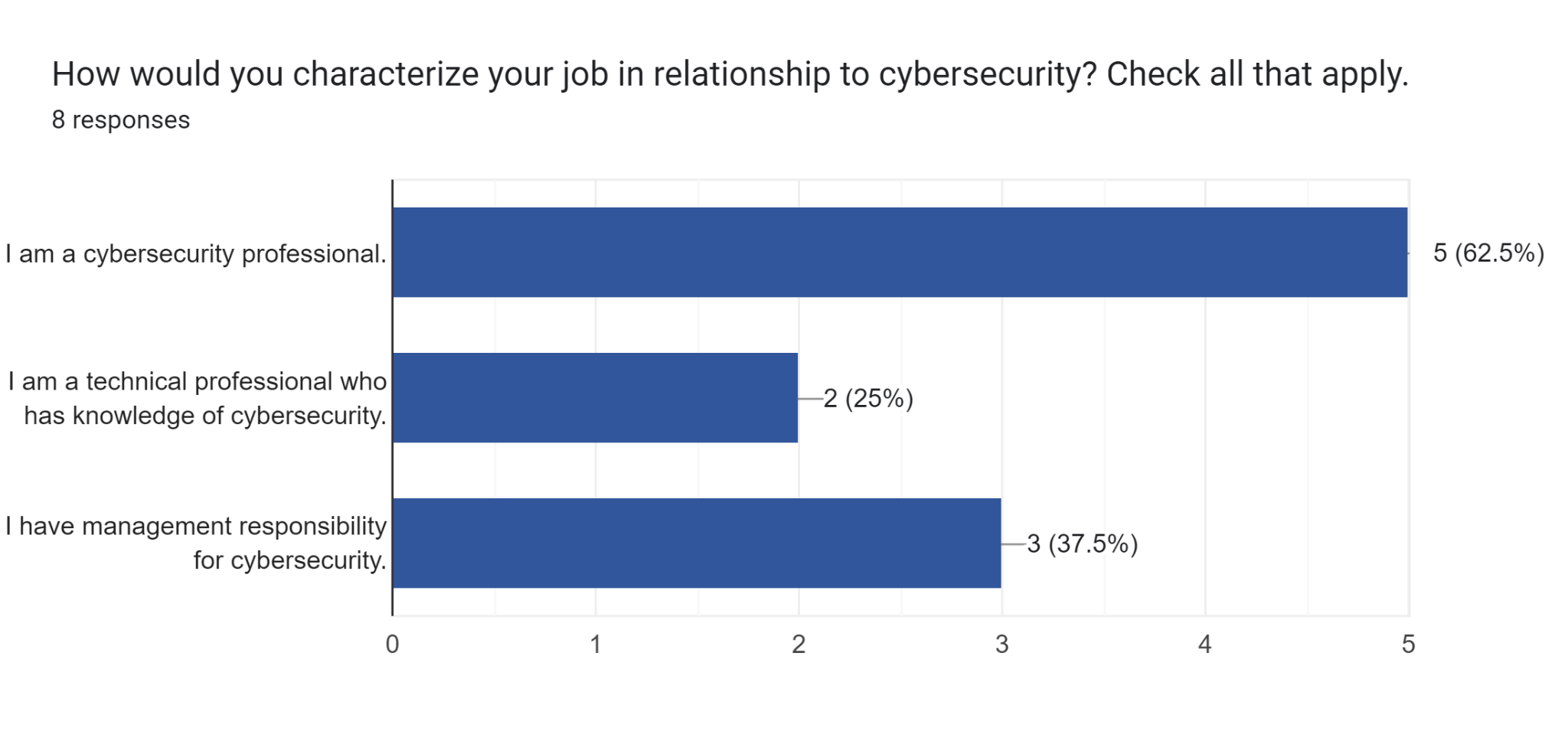
# Appendix E: Attendee Survey Report

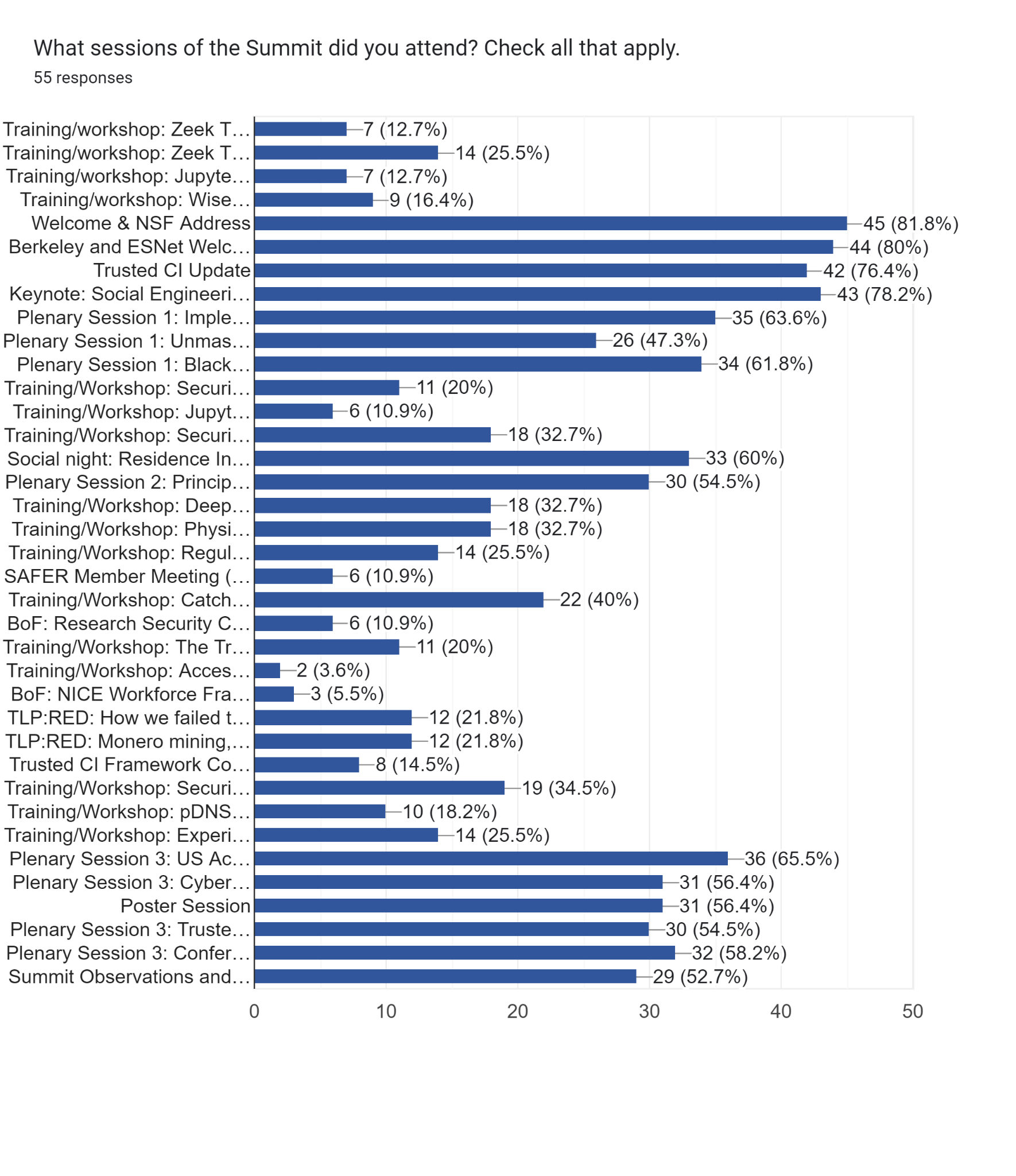
Below are the collected responses from the Summit Attendee Survey, displayed as charts.

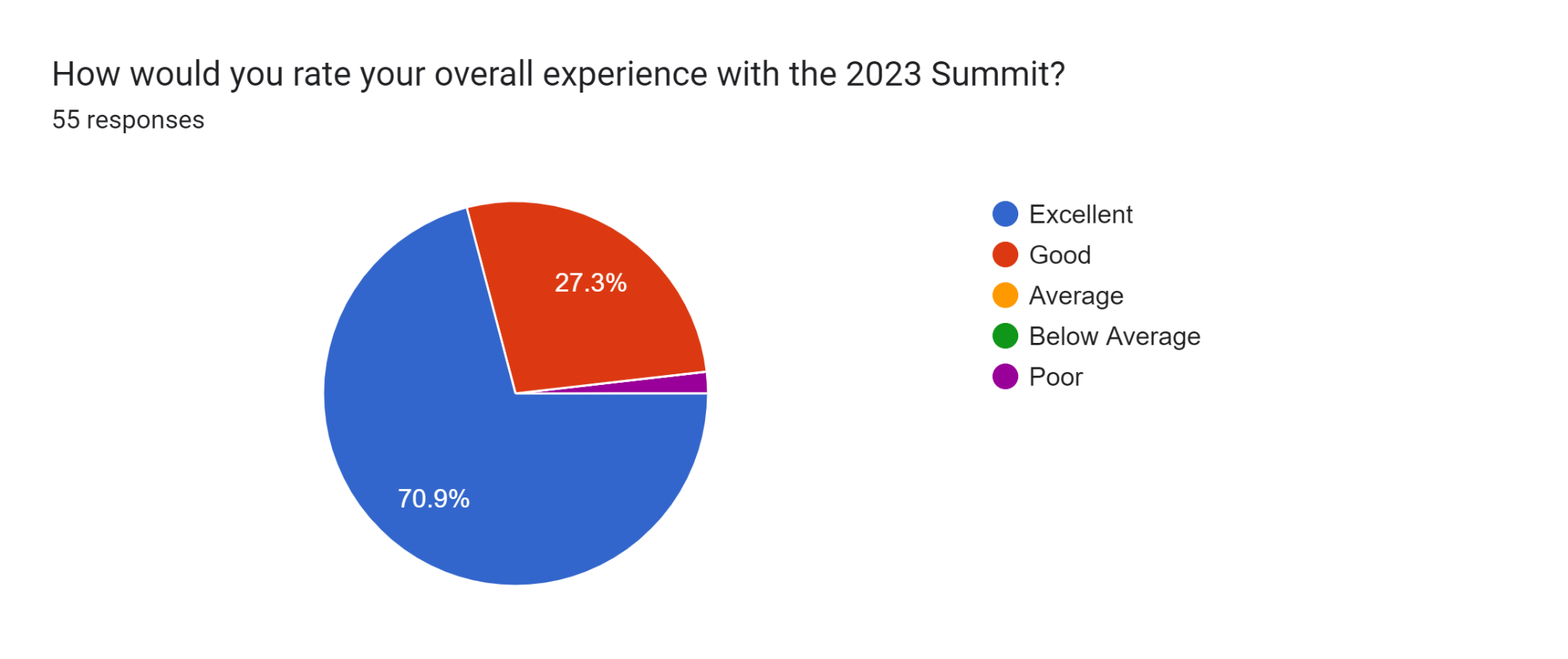


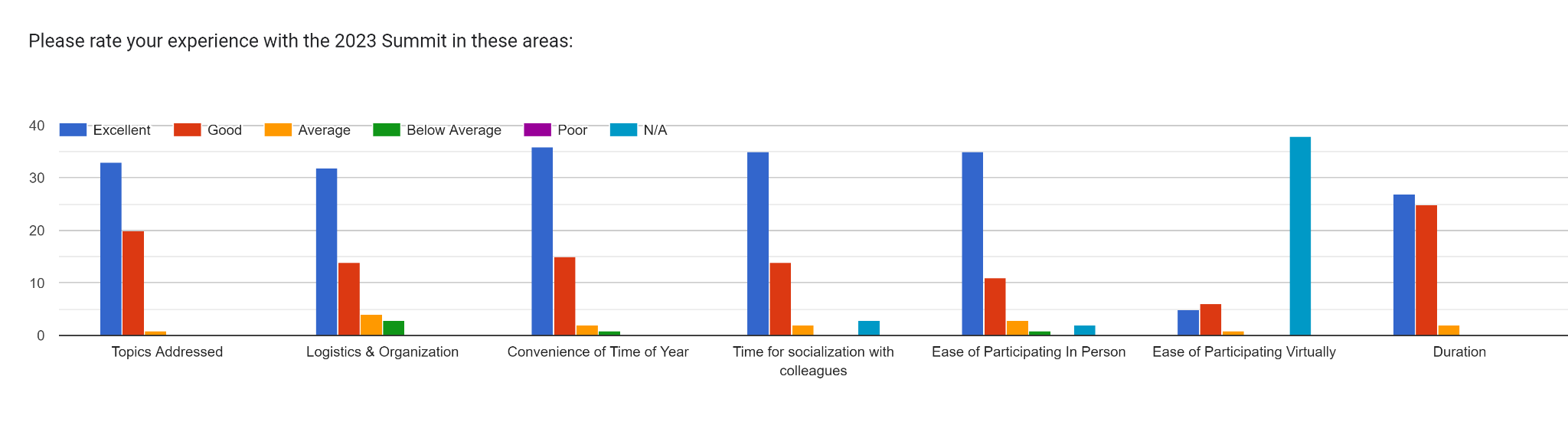


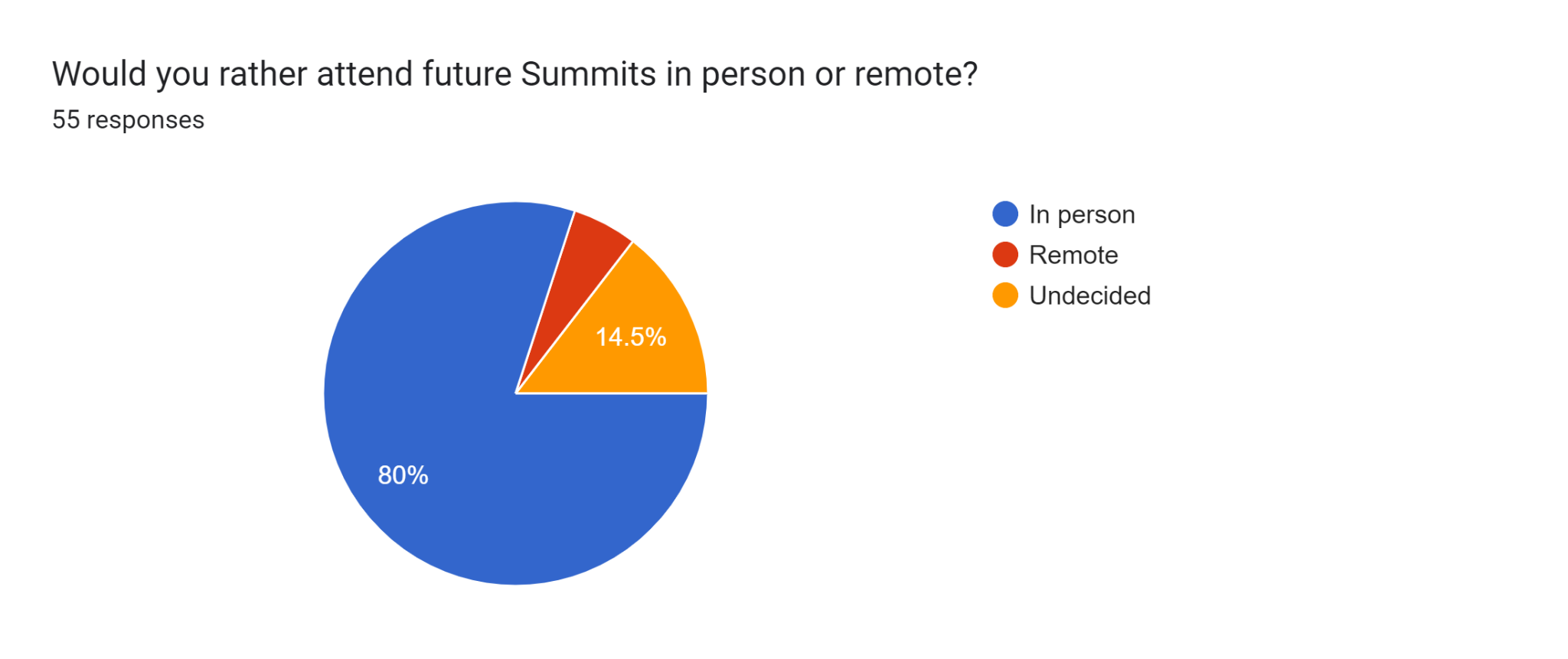


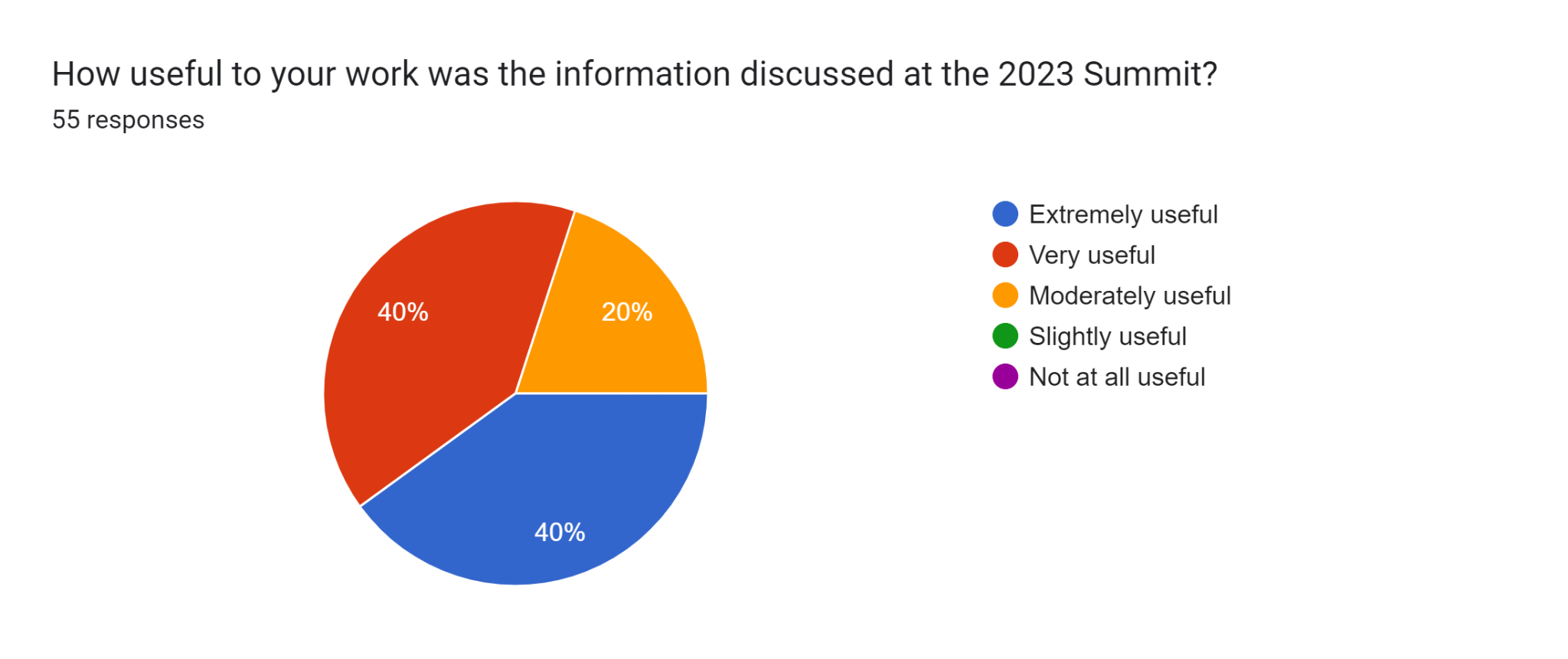


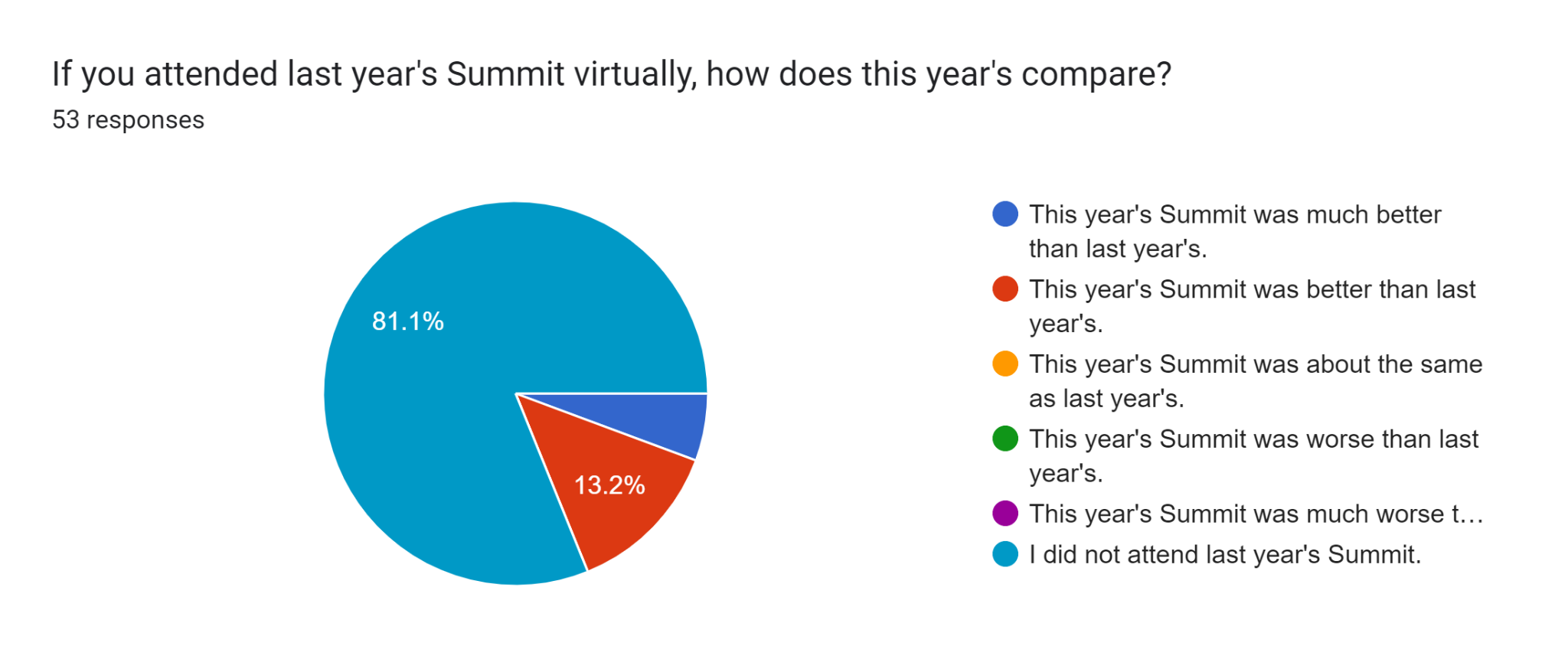




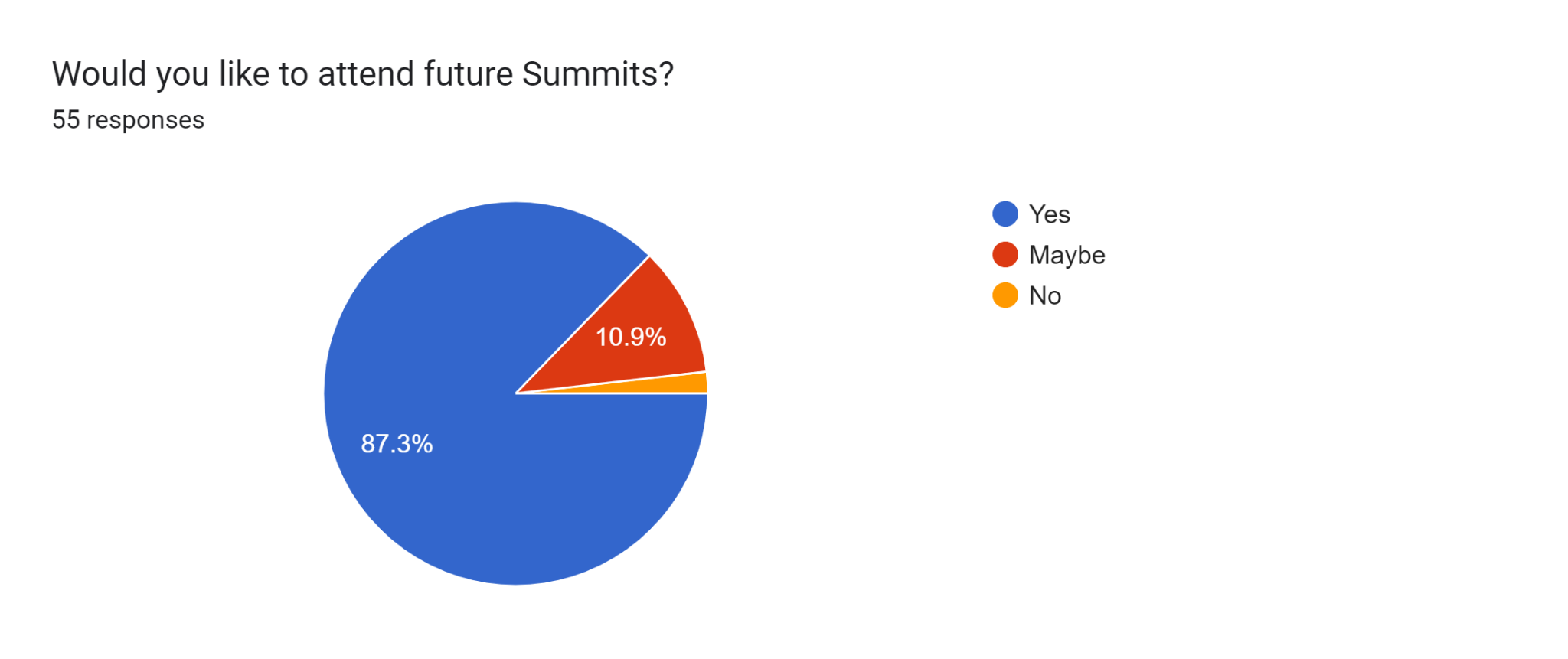








Forms response chart. Question title: How important is it that future Summits support remote attendees?
. Number of responses: 55 responses.



1. Presenter affiliation and job title can be found in *Appendix B: Speakers and Trainers.* [↑](#footnote-ref-1)
2. Gender Information was gathered via poll after Summit this year, so there were no opportunities for counting the number of people who skipped the question. [↑](#footnote-ref-2)