The Report of the 2022 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure

October 18-20, 2022

Hosted as an in-person and virtual conference

https://www.trustedci.org/2022-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 2022 Program Committee (highlighted in *Section 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 2022 NSF Cybersecurity Summit for Cyberinfrastructure and Large Facilities.

License

For the latest information on the Summit, please see: https://trustedci.org/summit/

Executive Summary

The *2022 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure* continued a ten-year 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, and in 2022, Trusted CI celebrated the 10th anniversary of hosting the Summit.

The 2022 Summit was back in person again in Bloomington, IN, October 18-20. A virtual option was available for Plenary 1 and 2. Please see *Appendix A* for the full *Summit Agenda*.

Framework adoption, Operational Technology, and preparing for AI were important themes at the Summit. Please see *Section 3 Common Themes and Challenges.*

The number of individuals who registered for the 2022 Summit was 224, including 17 students, and 12 of 17 NSF Large Facilities. Attendees enjoyed the in-person collaboration opportunities but continued to recognize the advantages of the virtual format.

International participation decreased from 11 countries in 2021 to four. The number of student attendees increased from 15 in 2021 to 17 this year. Please see *Appendix C* for information about the 2022 Summit student attendees.

Relevant content and relationship-building events resulted in an engaging and productive 2022 Summit. Survey responses from the attendees rated their overall experience with the 2022 Summit as Excellent or Good.

The Trusted CI team looks forward to an in-person 2023 Summit in Berkeley, CA, along with a virtual attendance option, so we can continue to advance the mission of the NSF science community.

1 Plenary Sessions[1]

1.1 Presentations

Slides provided by the presenters can be found here.

NSF Welcome: - *Robert Beverly*

Robert Beverly, NSF program officer with the Office of Advanced Cyberinfrastructure, praised the collaborative efforts of Trusted CI for its role over the past ten years as enablers of open and collaborative science. Unique challenges face scientific research, such as large instruments with big data and collaborative environments that are distributed geographically. All of the stakeholders must have data integrity.

Trusted CI, he said, continues to help organizations improve their CI as technology continues to evolve. He encouraged attendees to be mentors or mentees and to spread the word about CI and cybersecurity challenges and opportunities.

Cybersecurity: New Issues, Old Problems - *Helen Patton*

As the current chief information security officer (CISO) at Cisco and with previous high-level security positions at Ohio State and JP Morgan, Helen Patton brings perspective from three worlds: high tech, higher education, and finance. When she first went to Ohio State, she thought the CISO job would be easier. She soon found out that no matter where you are, cybersecurity is challenging, and it's hard to get decision makers to care about it and fund it.

Patton tackled the question of how to prepare for new technologies when IT professionals are having trouble protecting organizations from the current threats. Patton offered the following steps based on a Cisco study. Security should be based on enabling the business/research, managing the risk, and operating efficiently.

She named five practices that make a difference in a security program: proactive tech refresh, well integrated tech, timely incident response, prompt disaster recovery, and accurate threat detection.

Specifically, in regard to research, she said security needs a multidisciplinary approach that involves many groups within an organization, such as legal, IT, management, and scientists. Patton reminded attendees that the work they do to support research is ground zero for everything else in the academic arena.

[1] Presenter affiliation and job title can be found in *Appendix B: Speakers and Trainers.*

Trusted CI Update - *Jim Basney*

Jim Basney, director of Trusted CI, welcomed attendees and thanked all those who made the Summit possible. During the ten years that Trusted CI has hosted the Summit, it has become an annual event and attendance has grown. Basney thanked Von Welch, previous Trusted CI director, for his ten years of leadership and for charting a path for the next ten years. He also introduced Sean Peisart, the new deputy director of Trusted CI.

Ten years of collective knowledge and experience, along with input from the community, culminated in the production of the Trusted CI Framework. Now, more than half of NSF Major Facilities have adopted the Framework and are working with Trusted CI ambassadors dedicated to improving cybersecurity at their facilities. Trusted CI is expanding its focus to help programs of all sizes adopt the Framework.

The ten-year mark was also an opportunity to renew focus on Trusted CI's Fellows program. Each year, six Fellows are chosen from the scientific community to develop their cybersecurity knowledge. They become part of a diverse group of Fellows that champion cybersecurity in their scientific and geographic communities.

In his closing remarks, Basney encouraged attendees to stay connected to monthly webinars, and to make plans to attend the Summit in 2023 in Berkeley, CA.

Operations on the Security of Operational Technology in Scientific Research - *Emily K. Adams, Ryan Kiser, Mark Krenz, Sean Peisert*

Initial findings and recommendations were shared from the 2022 Trusted CI Annual Challenge on the Security of Operational Technology (OT) in Scientific Research.

1. In the first half of the year, the team conducted interviews with personnel involved with IT security and OT operations at a variety of NSF Major Facilities.
2. In the second half of the year, the team developed a forward-looking "Roadmap for Securing Operational Technology in NSF Scientific Research" to advance the security of scientific OT.
3. The team shared the observations and findings from conversations with NSF Major Facilities and NSF personnel, and provided preliminary elements of the roadmap they developed for release at the end of 2022.

ResearchSOC and CI Security Operations—What We've Learned - *Josh Drake*

ResearchSOC provides a community approach to cybersecurity. ResearchSOC:

1. Provides many advantages over security silos, such as reducing costs, understanding threats in research, evolving with each facility, career paths for SMEs, and learning together.
2. Offers many services when onboarding new facilities.

3. Has expertise in providing cybersecurity for the higher ed and research community and provides many resources.

Assurance Update - *Tom Barton*

An Executive Order in 2021 and subsequent Office of Management and Budget guidance obligated federal agencies to implement Zero Trust security architectures, joining the DoD's CMMCv2 and Confidential Unclassified Information as increasing levels of authentication and identity assurance requirements. Tom identified:

1. What's happening in response within the National Institute of Health and NSF.
2. How commercial services are responding.
3. Ways for research and education-focused organizations to comply with the new guidance.

Exploring Trust for Communities—Building trust for research and collaboration - *Maarten Kremers*

When exploring the intimidating world of federated identity, research communities can reap considerable benefit from using common best practices and adopting interoperable ways of working.

1. EnCo, the Enabling Communities task of the GÉANT 4-3 Trust and Identity Work Package, provides the link between those seeking to deploy federated identity management and the significant body of knowledge accumulated within the wider community, within projects and groups.
2. The presentation provided an overview on the linkages provided by research communities and their infrastructure services and the work they provide.

Supply Chain Attacks - *Theodore Pham*

The presenter used the Solar Winds hacker attack as a case study. Among lessons learned:

1. Defense in depth by slowing down the threat actor and giving detectors time to detect.
2. Security is a team sport. Everyone has a role in security.
3. Prep. Test your backups. Do tabletop exercises.

Implementing Federated Identity Management for Earth Science Data Access - *Doug Ertz, Rob Casey, Josh Drake, Erik Scott*

The SAGE and GAGE facilities began the process of merging two of NSF's Major Facilities in 2020. Among topics discussed:

1. The two facilities faced challenges designing and implementing an identity management system that supports the mission of their new facility and enables authenticated and auditable data access without becoming a barrier to researchers.
2. Lessons learned and challenges each facility encountered during the process discussed.

3. Resources available to the research community to solve identity management problems, such as the CI Compass and Trusted CI Federated Identity Management cookbook.

1.2 Panels

Lessons from the Trusted CI Framework Cohort
Moderator: *Scott Russell*
Panelists: *Jerry Brower, Wade Craig, Eric Cross, Doug Ertz, Craig Risien, and Randy Trudeau*

The Trusted CI Framework established a minimum standard for cybersecurity programs. With a lot of framework choices out there, why use this one?

1. Targeted at organizational leadership, the Framework is designed to support your mission and is built from Trusted CI's on-the-ground experience and R&D.
2. During the Framework Cohort, participants develop a validated assessment of their cybersecurity program with a timeline of milestones and draft a cybersecurity strategic plan that is tied to their mission.
3. The panelists discussed the benefits of participating with other Major Facilities over the six-month period.

Cybersecurity in a Large Research Facility (One Institution's Approach)
Moderator: *Joseph Brigham, David S. Butcher, Julia H. Smith*
Panelists: *Jim Berhalter, Abigail Centers*

The panel discussed lessons learned from Florida State University's National High Magnetic Field Laboratory (MagLab) on how to enhance cybersecurity in a large research facility. Critical success factors were:

1. Obtaining resources required to implement and maintain needed capabilities.
2. Interdisciplinary and diverse skill sets.
3. Phased implementation and understanding the allocation of responsibilities.

Trusted CI Fellows Panel
Moderator: *Rick Wagner*
Panelists: *Brian Roland, Charles McElroy, Garhan Attebury, Hannah Hiles, Joey White-Swift, Melissa Cragin, Stephen Streng, Unal Tatar*

2022 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.

1.3 Lightning Talks

1. **Trusted AI –** *Paul Brenner*
2. **Understanding the role of cyber hygiene in target suitability –** *Harsh Parekh*
3. **Enumerating non-malicious & malicious threats to scientific workflow integrity –** *Emily K. Adams, Brian Chase*
4. **Your screenshots tell more than you think: Privacy leakage in screenshots shared over Twitter –** *Yunhe Feng*
5. **A data anonymization proxy for interactive log analyses –** *Phuong Cao*

2 Realtime Training and Workshop Descriptions

Token-based Authentication and Authorization - *Derek Simmel, Jim Basney*

Discussion on development of interoperable solutions, best practices for token handling, and security requirements for trust and operations through token lifecycles.

Regulatory Compliance for Research: DFARS, CMMC, CUI, HIPAA, GDPR, NSPM-33 - *Anurag Shankar, Will Drake and Scott Russell*

Discussion of types of compliance, when you need it and when you don't, trend lines, privacy, government expectations, and a roadmap on how to get started on compliance.

Secure Programming and Dependency Analysis Tools - *Elisa Heymann, Barton Miller*

Discussion on making cloud/grid software more secure, tutorials, automating in-depth assessments, and improving the quality of automated code analysis.

Command Line Security - *Mark Krenz, Ishan Abhinit*

Discussion on the popularity of command line security and its wide use in academics and research.

Cybersecurity With Machine Learning - *Rajvardhan Oak*
Discussion of machine learning basics and applications, anomaly detection, and spam detection.

SP 800-82r3 says that OT is the new ICS/SCADA - *Philip Salkie*

Discussion of the difference between IT and OT and why the IT team should not be responsible for OT security. Securing OT needs a business plan, a budget, and a multidisciplinary approach.

Physical Security is Important Um'k - *Adrian Crenshaw, Mike Simpson*

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.

Security Log Analysis - *Mark Krenz, Ishan Abhinit*

Discussion centered on log analysis issues and log sources, log intelligence, and log data enrichment, event management, analysis, and response.

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

Discussion on how to adopt and implement the Trusted CI Framework.

Designing, executing, and maximizing the value of your tabletop security exercises - *Josh Drake, Ryan Kiser, Brian Chase*

Instructors helped participants improve their tabletop security exercise programs.

3 Common Themes and Challenges

Framework adoption, Operational Technology, and preparing for AI were important themes at 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 2022 Summit included:

- Framework adoption
- Operational Technology
- Preparing for AI
- Identity and access management
- Compliance challenges
- Risk assessment and management

4 Summit Management and Planning

The 2022 Summit was organized and hosted by Trusted CI, the NSF Cybersecurity Center of Excellence. Several staff members from Indiana University's CACR organized the Summit. Diana Cimmer, project management specialist, provided overall leadership for the Summit. The Organizing Committee included: Leslee Bohland, administrative director; Kelli Shute, executive director; and Cory Gleyze, security analyst.

A Program Committee (PC) comprised key leaders from NSF CI projects and the broader community. The PC was charged with five core tasks for 2022: (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, and Anita Nikolich served as co-chair. The PC held 11 meetings by Zoom beginning March 7, 2022 and ending July 14, 2022. It conferred electronically prior to and following this time period.

The 2022 PC members were:

- **James Marsteller (Chair) -** retired
- **Anita Nikolich (Co-chair)** - director of Research and Technology Innovation and research scientist, University of Illinois Urbana-Champaign
- **Chris Morrison** - head of Information Technology Operations, NSF's NOIRLab
- **Aunshul Rege** - associate professor with the Department of Criminal Justice, Temple University
- **Stan Waddell** - vice president for Information Technology and CIO, Carnegie Mellon
- **Hoda Maleki** - assistant professor, Augusta University
- **Fatema Bannat Wala -** security engineer, ESnet

The PC's 2022 CFP maintained 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 and lightning talk proposals that focused on NSF Major Facilities' unmet cybersecurity challenges, lessons learned, and/or significant successes. Training 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 2022 Summit was 224 including 17 students. 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 from the previous high of 11 in 2021. The number of student attendees increased from 15 in 2021 to 17 this year. Please see *Appendix C* for information about the 2022 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	2022	2021	2020	2019	2018
White or Caucasian	126 (56.3%)	191 (58.0%)	141 (49.5%)	88 (57.9%)	84 (71.2%)
Asian or Southeast Asian	32 (14.3%)	41 (12.5%)	28 (9.8%)	16 (10.5%)	8 (6.8%)
Prefer not to answer	10 (4.5%)	17 (5.2%)	15 (5.2%)	6 (3.9%)	7 (5.9%)
Hispanic or Latino	12 (5.4%)	14 (4.3%)	15 (5.2%)	7 (4.6%)	1 (0.8%)
Black or African American	6 (2.7%)	8 (2.4%)	16 (5.6%)	6 (3.9%)	1 (0.8%)
Multiracial	2 (0.9%)	6 (1.8%)	5 (1.8%)	3 (2.0%)	2 (1.7%)
Other Ethnicity	2 (0.9%)	1 (0.3%)	1 (0.4%)	0 (0%)	1 (0.8%)
Middle Eastern	0 (0%)	1 (0.3%)	1 (0.4%)	0 (0%)	0 (0%)
No Answer Provided	34 (15.2%)	50 (15.2%)	63 (22.1%)	26 (17.1%)	14 (11.9%)

Table 2. Attendee self-reported gender.[3]

Gender / Sex	2022	2021	2020	2019	2018
Female	44 (19.6%)	68 (20.7%)	36(35.2%)	27 (17.8%)	18 (15.3%)
Male	138 (61.6%)	201 (61.1%)	68(66.7%)	96 (63.2%)	75 (63.6%)
No Answer Provided	32 (14.3%)	57 (17.3%)	N/A[2]	28 (18.4%)	25 (21.2%)
Non-Binary	0 (0.0%)	3 (0.9%)	1(1.0%)	1 (0.7%)	0 (0%)
Gender Non-Conforming	1 (0.0%)				
Prefer not to answer	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 40 responses to the Summit Attendee Survey.

[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.

Of 40 respondents, 39 rated their overall experience with the 2022 Summit as Good or Excellent. A large majority, 28 of 40, said they would like to attend future Summits in-person, six of 40 said remote, six were undecided. Of the 40 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 *2022 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 39 of 40 attendees rated their overall experience with the 2022 Summit as Excellent or Good. Summit participants valued content addressing current issues, such as Framework adoption, Operational Technology, and preparing for AI. The Trusted CI team looks forward to serving the NSF science community with an in-person meeting for the 2023 Summit along with a virtual attendance option.

Appendix A: Summit Agenda

PROGRAM AGENDA

2022 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure

Program Committee Members:
Jim Marsteller (chair), Anita Nikolich (co-chair), Chris Morrison, Aunshul Rege, Hoda Maleki, Stan Waddell, Fatema Bannat Wala

Organizers:
Diana Cimmer (lead), Leslee Bohland, Kelli Shute,Cory Gleyze

All Times Listed in Eastern Daylight Time (EDT)

PLENARY SESSION 1

Wednesday, October 19, 2022
Slides provided by the presenters can be found here.

Time	Session title
8-9 am	**Sign-in and Continental Breakfast**
9 am	**Welcome and NSF Address** (*Rob Beverly)*
9:15 am	**Cybersecurity: News Issues, Old Problems** (*Helen Patton*)
10:15 am	**Trusted CI Update** (*Jim Basney*)
10:35 am	**Break**
11 am	**Student Introduction**
11:30 am	**Lightning Talks**
12-1:30 pm	**Lunch and Table Talks**
1:30 pm	**Observations on the Security of Operational Technology in Scientific Research** (*Emily K. Adams, Ryan Kiser, Mark Krenz, Sean Peisert)*
2 pm	**Lessons from the Trusted CI Framework Cohort** (*Scott Russell, Jerry Brower, Wade Craig, Eric Cross, Doug Ertz, Craig Risien, and Randy Trudeau)*

3 pm	**Cybersecurity in a Large NSF Research Facility (One Institution's Approach)** (*Joseph Brigham, David S. Butcher, Julia H. Smith, Jim Berhalter, Abigail Centers)*
4 pm	**Break**
4:30 pm	**ResearchSOC and CI Security Operations—What We've Learned** (*Josh Drake*)
5 pm	**Adjourn**
6-9 pm	**Social at Nick's English Hut**

PLENARY SESSION 2

Thursday, October 20, 2022

Time	Session title
8-9 am	**Sign-in and Continental Breakfast**
9 am	**Trusted CI Fellows Panel** (*Rick Wagner, Brian Roland, Charles McElroy, Garhan Attebury, Hannah Hiles, Joey White-Swift, Melissa Cragin, Stephen Streng, Unal Tatar)*
10 am	**Assurance Update** *(Tom Barton)*
10:30 am	**Exploring Trust for Communities—Building Trust for Research and Collaboration** *(Maarten Kremers)*
11 am	**Supply Chain Attacks** (*Theodore Pham*)
11:30 am - 12 pm	**Break**
12 pm	**Implementing Federated Identity Management for Earth Science Data Access** *(Doug Ertz, Rob Casey, Josh Drake, Erik Scott)*
1 pm	**Open Discussion and Summary of Summit Findings**
1:30 pm	**Adjourn**

TRAINING DAY

Tuesday, October 18, 2022 (In-person only)

Time	Session title
9 am - 1 pm	**Token-based authentication and authorization** *Organizers: Derek Simmel, Jim Basney*
9 am - 1 pm	**Regulatory Compliance for Research** *Instructors: Anurag Shankar, Will Drake, Scott Russell*
9 am - 1 pm	**Secure Programming and Dependency Analysis Tools** *Instructors: Elisa Heymann, Barton Miller*

9 am - 1 pm	**Command Line Security** *Instructors: Mark Krenz, Ishan Abhinit*
9 am - 1 pm	**Cybersecurity with Machine Learning** *Instructors: Rajvardhan Oak*

Time	Session title
2-6 pm	**Token-Based Authentication and Authorization** *Instructors: Derek Simmel, Jim Basney, Brian Bockelman, Derek Weitzel*
2-6 pm	**SP 800-82r3 says that OT is the new ICS/SCADA** *Instructors: Philip Salkie*
2-6 pm	**Security Log Analysis** *Instructors: Mark Krenz, Ishan Abhinit*
2-6 pm	**The Trusted CI Framework: Strategies for Getting Started** *Instructors: Scott Russell, Craig Jackson*
2-6 pm	**Designing, Executing, and Maximizing the Value of your Tabletop Exercises** *Instructors: Josh Drake, Ryan Kiser, Brian Chase*

Appendix B: Speakers and Trainers

Name	Institution	Job Title
Ishan Abhinit	Indiana University, Center for Applied Cybersecurity Research	Senior Security Analyst
Emily K. Adams	Indiana University, Center for Applied Cybersecurity Research	Principal Security Analyst/CISO
Garhan Attebury	University of Nebraska-Lincoln	Lead System Administrator- (Fellows)
Tom Barton	University of Chicago	Senior Director and CISO
Jim Basney	National Center for Supercomputing Applications, Trusted CI	Director, Trusted CI
Joseph Brigham	Florida State University	Program Director
Robert Beverly	NSF Office of Advanced Cyberinfrastructure	Program Officer
Jim Berhalter	Florida State University	IT Manager
Brian Bockelman	Morgridge Institute for Research	Investigator, Research Computing
Paul Brenner	The University of Notre Dame	Senior Associate Director
Jerry Brower	NOIRLab-Gemini Observatory	Information Security Officer
Phuong Cao	National Center for	Cybersecurity Specialist

	Supercomputing Applications	
Rob Casey	IRIS	Deputy Director Cyberinfrastructure
Brian Chase	Indiana University, OmniSOC/ ResearchSOC	Security Analyst
Melissa Cragin	San Diego Supercomputer Center at the University of California San Diego	Chief Strategist for Data Initiatives in the Research Data Services (Fellows)
Wade Craig	NRAO	Cybersecurity Specialist
Adrian Crenshaw	ResearchSOC	Analyst
Abigail Centers	Florida State University	Research Assistant
Jeannette Dopheide	National Center for Supercomputing Applications, University of Illinois, Trusted CI	Senior Education, Outreach, and Training Coordinator
Josh Drake	Indiana University, OmniSOC/ResearchSOC	Security Services Manager
Will Drake	Indiana University, Center for Applied Cybersecurity Research	Chief Information Security Officer
Doug Ertz	UNAVCO, Inc.	Project Manager
Yunhe Feng	University of Washington	Postdoctoral Scholar
Elisa Heymann	University of Wisconsin-Madison	Senior Scientist
Hannah Hiles	RENCI	Research Project Manager and Product Owner (Fellows)
Craig Jackson	Indiana University, Center for Applied Cybersecurity Research	Program Director
Ryan Kiser	Indiana University, OmniSOC/ResearchSOC	Senior Security Analyst
Maarten Kremers	SURF	Technical Product Manager
Mark Krenz	Indiana University, Center for Applied Cybersecurity Research	Lead Security Analyst
Charles McElroy	Cleveland State University	Assistant Professor (Fellows)
Bart Miller	University of Wisconsin-Madison	Professor
Helen Patton	CISCO	CISO
Sean Peisert	Lawrence Berkeley National Laboratory	Staff Scientist
Theodore Pham	Carnegie Mellon University	Director, Information Security Information Security Office
Craig Risien	Oregon State University	Senior Faculty Research Assistant
Brian Roland	Northwestern University	Data Management Specialist (Fellows)

Scott Russell	Indiana University, Center for Applied Cybersecurity Research	Senior Policy Analyst
Philip Salkie	Jenariah Industrial Automation	Manager
Eric Scott	RENCI	Senior Research Software Developer
Anurag Shankar	Indiana University, Center for Applied Cybersecurity Research	Senior Security Analyst
Derek Simmel	Pittsburgh Supercomputing Center	Senior Information Security Officer
Mike Simpson	Indiana University, OmniSOC/ResearchSOC	Senior Security Analyst
Julia H Smith	Florida State University	Field Research Faculty
Stephen Streng	University of Minnesota	Research Development Strategist with Strategic Projects and Research Collaborative (Fellows)
Unal Tatar	SUNY at Albany	Assistant Professor (Fellows)
Randy Trudeau	Caltech	Information Security Officer
Rick Wagner	University of California San Diego	Systems Integration Engineer
Derek Weitzel	University of Nebraska - Lincoln	Research Assistant Professor
Joseph White-Smith	University of Texas at Dallas	Systems Engineer for HPC/CI in the Office of Information Technology (Fellows)

Appendix C: Student Participation

Ten students joined the Summit for three days of hands-on training, talks, panels, and active Q&A sessions. The following students agreed to share their names and institutions in the Summit report.

Name	Institution
Jacob Abbott	Indiana University
Jessy Ayala	UC Irvine
Tria Correll	Middle Georgia State University
Xinyao Ma	Indiana University
Rajvardhan Oak	UC Davis
Harsh Parekh	Louisiana State University
Mahmoud Shabana	New York University
Joshua Thornburgh	University of Arkansas
Alexs Wijoyo	Pace University
Alenna Zweiback	Indiana University

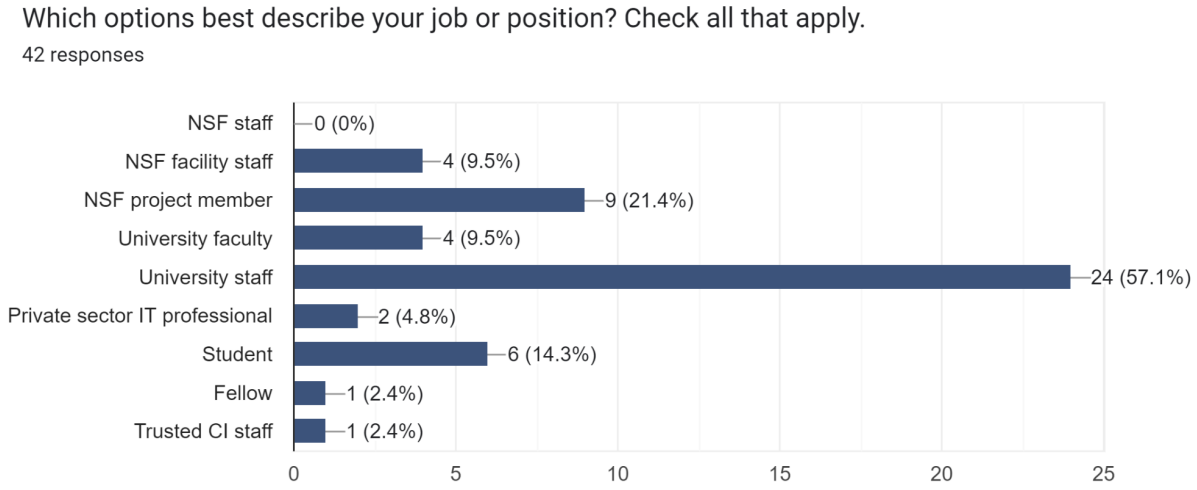
Appendix D: NSF Project Representation

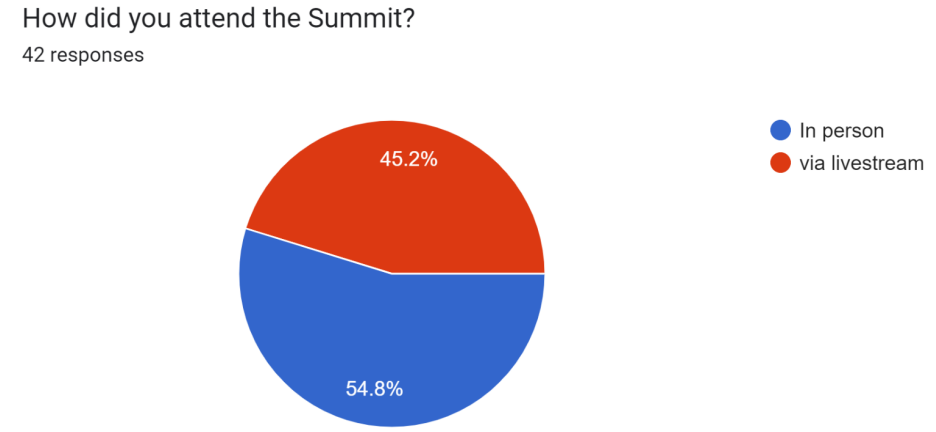
The 12 NSF Large Facilities represented at this year's Summit were:

- Academic Research Fleet
- Icecube Neutrino Observatory
- International Ocean Discovery Program
- Large Hadron Collider
- Laser Interferometer Gravitational-wave Observatory
- Geodetic Facility for the Advancement of Geoscience
- Seismological Facility for the Advancement of Geoscience
- National High Magnetic Field Laboratory
- NSF's National Optical-Infrared Astronomy Research Laboratory
- National Radio Astronomy Observatory
- National Solar Observatory, Daniel K Inouye Solar Telescope
- Ocean Observatories Initiative

Appendix E: Attendee Survey Report

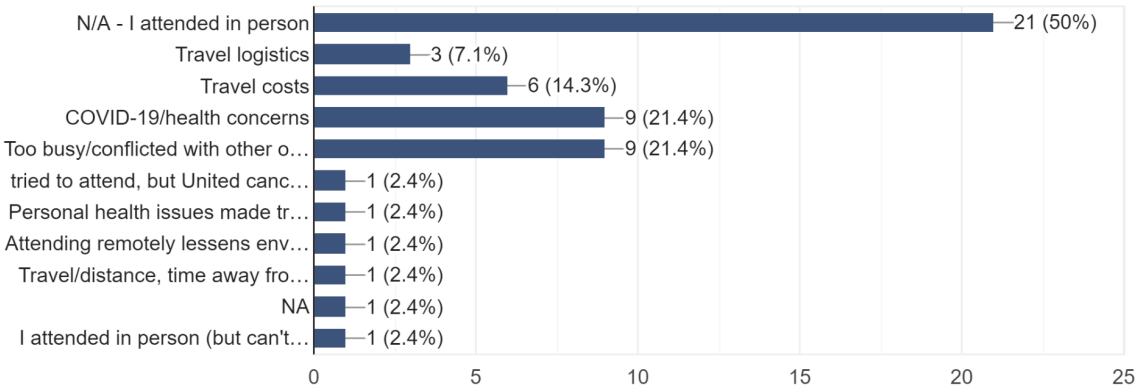
Below are the collected responses from the Summit Attendee Survey, displayed as charts.





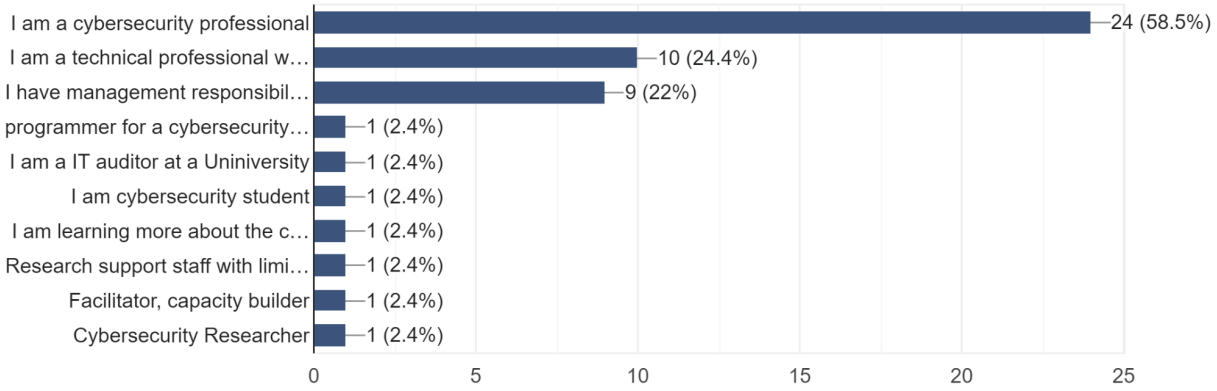
What factors kept you from attending in person? Check all that apply.

42 responses



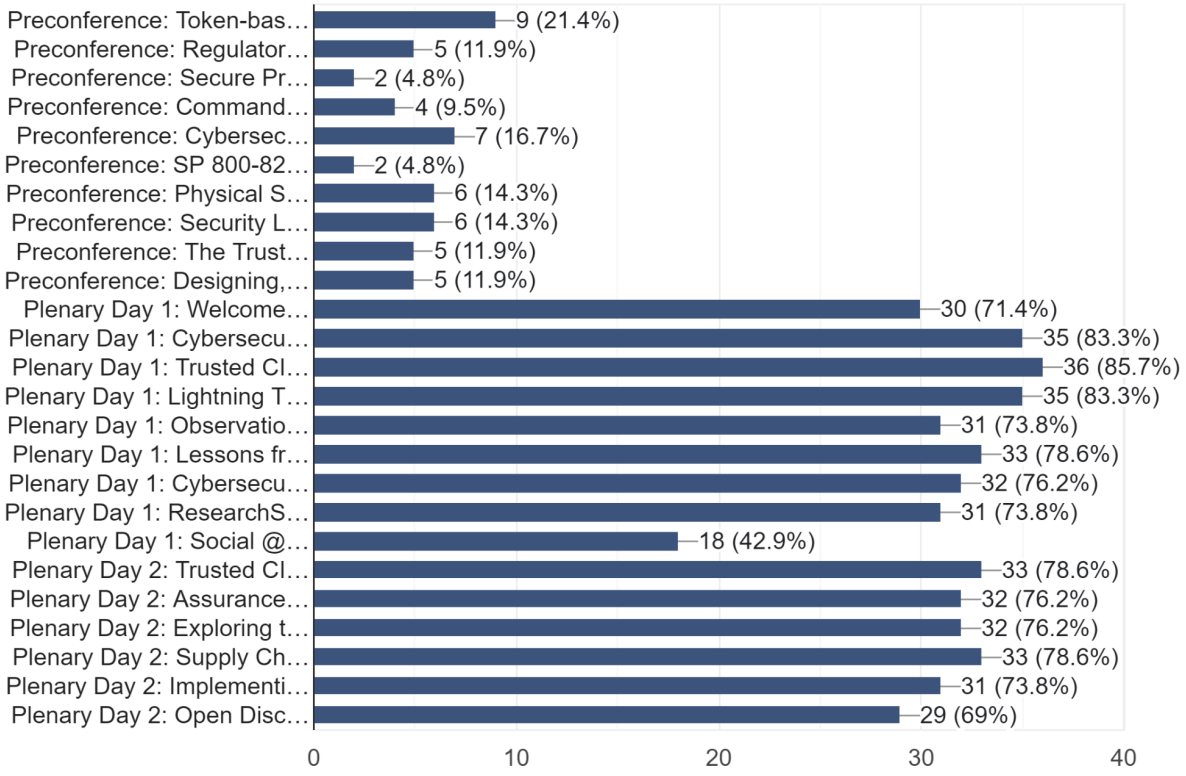
How would you characterize your job in relationship to cybersecurity? Please check all that apply.

41 responses



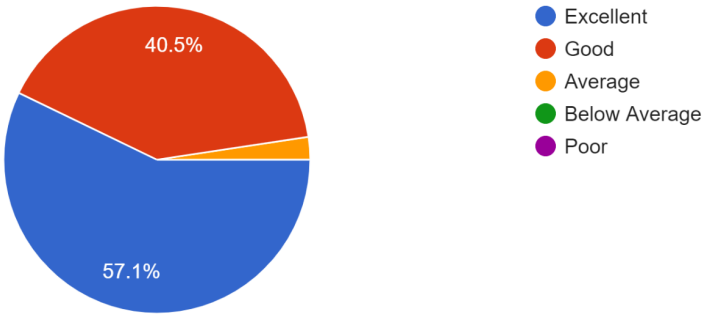
What sessions of the Summit did you attend? Check all that apply.

42 responses

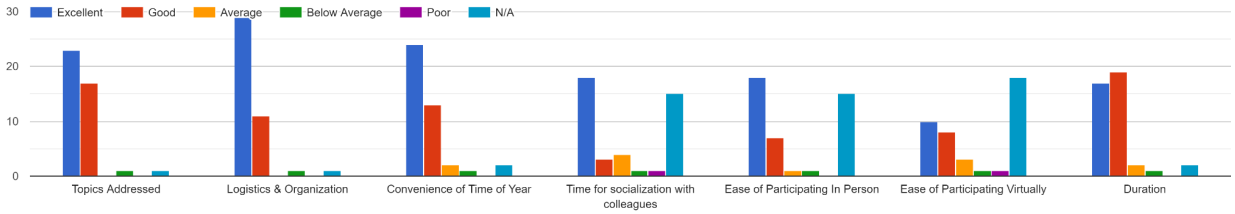


How would you rate your overall experience with the 2022 Summit?

42 responses

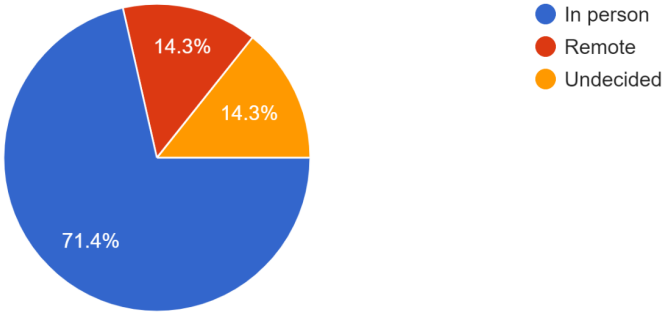


Please rate your experience with the 2022 Summit in these areas:



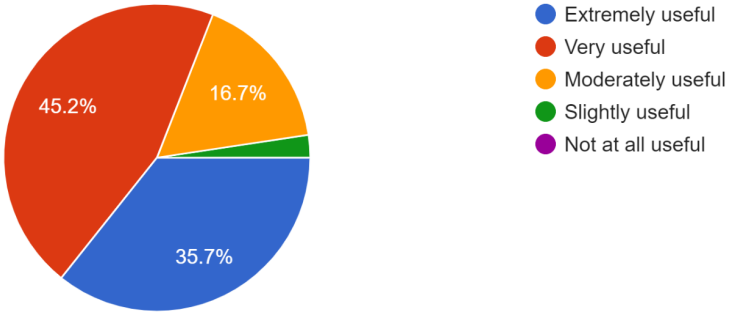
Would you rather attend future Summits in person or remote?

42 responses



How useful to your work was the information discussed at the 2022 Summit?

42 responses

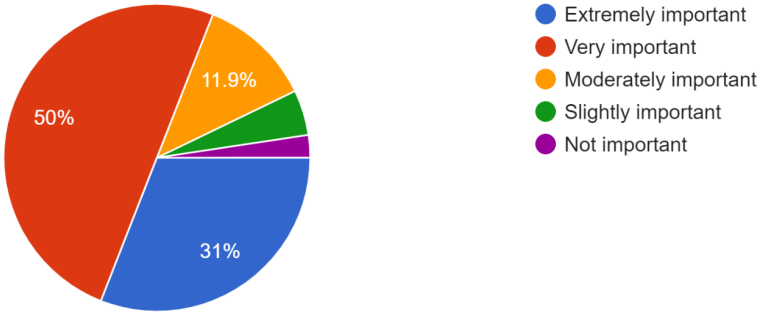


If you attended last year's Summit virtually, how does this year's compare?

42 responses

How important is it that future Summits support remote attendees?

42 responses



Would you like to attend future Summits?

42 responses