

The Report of the
2018 NSF Cybersecurity Summit for
Large Facilities and Cyberinfrastructure

August 21 - 23, 2018

Westin Alexandria - Alexandria, VA

<https://trustedci.org/2018nsfsummit/>

Acknowledgements

The organizers wish to thank all those who attended the summit. Special gratitude goes to all those who responded to the CFP, spoke, provided training, and actively participated, including the 2018 Program Committee (highlighted in [Section 5](#)), without whom the event would not have been as successful. Our sincere thanks goes to the National Science Foundation and Indiana University's Center for Applied Cybersecurity Research for making this community event possible.

This event was supported in part by the National Science Foundation under Grant Number 1547272. 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 National Science Foundation.

About this Report

This document is the product of Trusted CI: The NSF Cybersecurity Center of Excellence and was supported by the National Science Foundation under the grant - ACI-1547272.

Citing this Report

Please cite as: Andrew Adams, Jeannette Dopheide, Mark Krenz, James Marsteller, Von Welch, and John Zage. Report of the 2018 NSF Cybersecurity Summit for Cyberinfrastructure and Large Facilities: <http://hdl.handle.net/2022/22588>.

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://trustedci.org/summit/>

Table of Contents

Executive Summary	4
1 Background: Evolving Cybersecurity Landscape, and Advancing Trustworthy Science	5
2 The Summit’s Purpose, Scope, and Theme	6
3 Summit Program Summaries	7
4 Community Observations and Future Challenges	11
4.1 Findings	11
4.1.1 Trust Relationships	11
4.1.2 Human factors	11
4.1.3 Positive Cybersecurity Metrics	11
4.1.4 Summit Impact	12
4.2 Observations	12
5 The Organizing and Program Committees	13
6 The Call for Participation	14
7 Summary of Attendees	15
7.1 NSF Project Representation	16
7.2 Student Representation	19
7.3 Inclusiveness	20
8 Attendee Evaluations	21
9 Conclusion	22
Appendix A: Recommendations From Past Summits	24
2017 Recommendations:	25
2016 Recommendations:	25
2015 Recommendations:	27

2014 Recommendations:	28
2013 Recommendations:	29
Appendix B: Descriptions of Workshops and Training Sessions	31
Concurrent Morning Sessions	32
Concurrent Afternoon Sessions	36
Appendix C: Summit Agenda	39
2018 NSF Cybersecurity Summit Agenda	40
August 21st- Training Day	40
August 22nd- Plenary Day 1	40
August 23rd - Plenary Day 2	41
Appendix D: Bios for Speakers, Program Committee, and Organizers	43
Bios for Speakers, Authors, Program Committee Members, Organizers, and Student Awardees	44
Appendix E: Student Feedback	59
Final Thoughts on Attending the Summit	60
Sanchari Das:	60
Grant Allard:	61
Preston Ruff:	61
Maggie Ahern:	61
Leah Dorman:	62
Appendix F: Attendee Survey Summary Report	64
Appendix G: Training Evaluation Summary Report	71

Executive Summary

The 2018 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure promoted a platform where communities with interest in supporting NSF science projects collaborated to address core cybersecurity challenges. The 2018 summit achieved this through the active participation of its community members. The community responded to the summit's call for participation (CFP) with thirty-two proposals consisting of fourteen plenary topics, eight training sessions, eight student applications and two table talks.

In Alexandria, VA the 2018 summit took place August 21st through midday August 23rd. As with previous summits, a full day of training and focused workshops, including a full day WISE (Wise Information Security for collaborating E-infrastructures) Community¹ training event, was offered on the first day. The second and third days followed a plenary model, offering a single track of presentations, panels and keynotes that focused on the security of cyberinfrastructure projects and Large Facilities.

The summit was attended by 117 individuals, with over half not having attended the summit in 2017. 31% of the attendees actively participated in either the planning, presenting, providing training, co-authoring a CFP submission, and/or leading a lunch table talk. Moreover, fifty-five NSF-funded projects were represented, including twenty-one Large Facilities. Based on the evaluations and feedback received, the attendees expressed overwhelmingly positive and constructive feedback.

In the course of the plenary, the 2018 summit identified future challenges for the NSF community. A full list of findings and future challenges is delineated in Section 4 of this report, with the following key observations derived from this year's summit:

Observation 1: The NSF Large Facilities and cyberinfrastructure members can benefit from stronger trust communities in order to share sensitive security information. This requires re-evaluating how current trust relationships are established, as well as how information is shared between community members.

Observation 2: The human factor in security events is continually overlooked. The community needs to better understand the interaction between humans and security, and to explore the possibility of users taking a larger role in security solutions.

Observation 3: Cybersecurity needs positive or proactive metrics, as opposed to presenting negative events and the risks associated with the lack of cybersecurity. Historically, the efficacy of security mechanisms has been presented in terms of attacks thwarted, e.g., the firewall has

¹ <https://wise-community.org/>

blocked n malicious packets, rather than in terms of positive productivity, e.g., n users accessed the database without complications.

1 Background: Evolving Cybersecurity Landscape, and Advancing Trustworthy Science

Trusted CI, now in its sixth year, organizes the annual NSF cybersecurity summit as a means to advance the NSF cybersecurity community and increase trust in the science supported by that community. The summit serves as a valuable tool for securing NSF scientific cyberinfrastructure (CI) and increasing trust in the science it supports by providing a forum for education, sharing of experiences, and community building. For many attendees, the summit is an opportunity to meet with colleagues, to benchmark and debate cybersecurity best practices, and to receive practical, relevant training.

The summit offers a forum for community members to share experiences, identify common challenges, and connect professionally. Moreover, the summit presents an excellent opportunity to highlight cybersecurity challenges to NSF program officers, leadership, and stakeholders, as well as provide basic cybersecurity awareness and education. Finally, the summit presents an opportunity for Trusted CI to gain insight into the needs, concerns, and challenges facing the community.

The constantly changing state of cybersecurity challenges is one that can be difficult for any organization, whether commercial, academic or governmental. During the summit opening, the Deputy Office Director of the Office of Advanced Cyberinfrastructure (OAC), Amy Friedlander, emphasized the importance of ongoing training and learning, as well as professional development. She also mentioned that cybersecurity is fundamental to the scientific research environment. Addressing the challenges of the ever-changing environment will be of central importance for the supporting and advancing of trustworthy science.

The 2018 summit took place August 21st through midday August 23th at the Westin Alexandria near NSF headquarters. On August 21th, the summit offered a full day of training that included a five parallel sessions in the morning and four parallel sessions in the afternoon. The second and third days followed a plenary format designed to highlight both the key cybersecurity issues facing Large Facilities and effective responses. The event brought together leaders in NSF CI and cybersecurity communities to continue the processes initiated in 2013: building a trusting, collaborative community, and addressing that community's core cybersecurity

challenges.

The remainder of this report is structured as follows: Section 2 outlines the summit's purpose, scope, and theme; Section 3 provides summaries of the presentations; Section 4 identifies the Findings, Recommendations, and Future Challenges identified from the Summit; Section 5 lists the organizing and program committee; Section 6 replicates the CFP and summit program; Section 7 provides details on the summit's attendance and participation; Section 8 provides the results of attendees' evaluations of the event; and Section 9 catalogues lessons learned. The report concludes with the closing thoughts of the organizers.

2 The Summit's Purpose, Scope, and Theme

The program committee decided to forego setting a theme for the 2018 summit. This decision would enable the community to decide the focus of the summit. An unofficial theme appeared across many of the presentations, that of sharing threat information and building stronger collaborations within the community. This was clearly evident in the panel *Incident Response Communications* that highlighted the need for better collaborations (see Section 3). The panelists discussed the problem with most information flows, i.e., closed communities lead to fragmented circulations of knowledge, and then suggested that it is as essential for information security analysts to build trust relationships within the community as it is for them to hone their technical skills.

Similarly, in the presentations *Responding to Advanced Threats as a Global Community* and *Silent Librarian* (see Section 3), Romain Wartel and Kim Milford, respectively, highlighted the need for those stronger trust relationships. Both talks discussed the profound realization that research and education cyberinfrastructure is a viable market for thieves, with Kim's talk additionally touching on the impetus of this new threat, namely monetized research.

The 2018 summit continued to build on the success, findings, and lessons learned from previous years.² This was discernible in the panel *Security Best Practices for Academic Cloud Service Providers* (see Section 3). Not only was the work inspired by multiple cloud-based presentations at the 2017 summit that touched on the challenges in securing cloud services, but it directly supported the summit's goal of identifying, establishing and sharing community standards for best practices regarding cybersecurity.

Measurable progress on the summits' other critical goals appeared in both the training sessions (see Appendix C) and plenary (see Section 3), specifically: providing pragmatic levels of

² See previous summit reports, agendas, and more at <https://trustedci.org/search?q=summit>

information security; meaningfully addressing software assurance, quality or supply chains in the context of the project cybersecurity programs; and supporting scientific discovery.

3 Summit Program Summaries

Biographies of speakers are included in Appendix D. Slides from the talks can be found at <https://iu.app.box.com/s/g2y4notvxoh5mgalnh5o79vjfe58bt6>.

Five Years Backwards and Forwards - Von Welch

Von Welch's keynote, unofficially titled *Cybersecurity: We don't have it right yet*, put forth the insight that security suffers from an inability to demonstrate its value, as well as presenting the notion that cybersecurity must keep a broad focus on all IT risks, not just those responsible due to malicious actors. He further explored the idea of re-examining the CIA triad (i.e., confidentiality, integrity and availability) for science and research, suggesting that efficient (available, collaborative and fast), trusted (integrity, quality assured and defensible) and reproducible reflect better the goals of science. The "reproducible" idea carried impact for the attendees for it reappeared in discussions throughout the summit.

Involving Students in Cybersecurity for CI - Jeremy Straub

NDSU offers cybersecurity graduate programs as well as summer camps for K-12. There are challenges to involving students, such as mitigating potential risk to opening infrastructure to students. However this creates opportunities for students to have experience in cybersecurity projects that are primarily for the student's experience or an unrelated project in which the student's experience is the secondary result. These student programs need to be exciting and informative while minimizing the potential for harm to the systems and work. Previous projects in NDSU include ethical hacking, CTF, and red vs blue challenges.

Security Best Practices for Academic Cloud Service Providers - Panel

Moderator: *Von Welch*

Panelists: *Rion Dooley and Mike Lowe*

Panelists' Rion and Mike presented the cumulative results, a list of best practices for academic cloud providers, from their collaborative endeavour featuring members from Agave, JetStream, Cornell, Cyverse and Trusted CI. The group worked together to tackle improving security for both cloud operators and users using a set of principles: security is a shared concern between a cloud service provider and a cloud service user, neither can expect the other to fully address security; a clean delineation between cloud service provider and cloud service user of security

responsibilities is critical to ensure all responsibilities are met; and the cloud service provider has the responsibility to ensure all security responsibilities are articulated and the cloud service user is educated about how to fulfill their responsibilities. These principles are significantly different from canonical best practices, which treat the user as the malicious actor rather than including the user in the security process.

Silent Librarian - Kim Millford and Brett Zupan

The three biggest types of attacks against academia are fake purchase orders, employment scans, and spoofed FBI and IRS calls extorting students. These attacks target data, people, or infrastructure. Silent Librarian gained attention due to the size of the attack. It was a series of over 750 phishing attacks conducted by Mabna Institute, stealing over 31 TB of data and costing an estimated \$3.4 billion according to the FBI. It targeted 144 US based universities, 176 foreign universities, and almost 50 domestic and foreign companies. It also targeted the states of Hawaii and Indiana, as well as the United Nations. 100,000 accounts associated with professors were targets, 8,000 which of those were compromised. The hackers sold both exfiltrated data and credentials, essentially monetizing research that was stolen. Investigations led to DOJ indictments and imposed sanctions. Recommended mitigations included using a defense-in-depth approach, quickly blocking or quarantining compromised hosts, dismissing the “I’m not a target” mentality, and committing to ongoing education for end-users.

Responding to Advanced Threats as a Global Community - Romain Wartel

Research and education institutions have allocated little money for protecting against well-financed attacks. This makes R&E a viable market for cybercriminals. A potential solution for obtaining quality and relevant threat intelligence is to share intel among the community. As an example, without threat sharing, malware waves can hit and last less than 4 hours, but antivirus vendors require more than 24 hours to detect these new strains and respond. With threat sharing, some of the threat can potentially be mitigated. One popular sharing network is MISP (Malware Information Sharing Platform).³

XSEDE Lessons Learned - Adam Slagell

A security incident was discovered impacting the XSEDE (<https://xsede.org/>) Single Sign On (SSO) Hub after discovering logs missing. The first action Adam took was to take the SSO hub offline. In this security incident, multiple sites were in play. There were issues getting updates posted, which were not sent out until the second day. The decision was made to rebuild the SSO Hub without home directories and to require 2FA, which was optional. Postmortem analysis revealed the incident started as a user account compromise and called into question

³ <https://www.misp-project.org>

the integrity of the logging system. Insights from the event included implementing a centralized syslog service, so security can get logs faster; however, such a system needs access control for the log servers.

Incident Response Communications - Panel

Moderator: *Susan Ramsey*

Panelists: *Ashwin Jacob Mathew, Dr. Daniel Massey, Adam Slagel, Romain Wartel and Kim Milford*

Ashwin Jacob Mathew presented the talk *Cooperation and Learning in Information Security* which broached one of the recurring concerns that cropped up in the summit, that of forming trust between information security analysts. Ashwin argued that most information flows exist within closed communities, which can lead to fragmented circulation of knowledge. Thus, information security analysts' responsibilities are as much about building relationships within the community as developing a skill set in security.

Upon the completion of Ashwin's presentation, moderator Susan Ramsey led the panelists on an exploration of the issues involved with building trust between federated security analysts. This resulted in the insight that perhaps the security community, and Security Operations Centers (SOCs) in general, need to re-evaluate the trust level and processes for sharing information, specifically, re-examining the benefit of sharing information with regards to risk.

Password Adventures for a VO - Warren Anderson

Over 1700 scientists in 105 countries are authorized through Kerberos for the LIGO.ORG realm. Initially, password quality policy was determined by what various IDM developers thought was appropriate at the time. This policy led to poor password management; passwords expired only when someone left, and password quality checking was not in place. The policy was updated to require users to update their passwords to new passwords within two weeks. Users had the option to set their own password with certain requirements or to use a preferred random password or passphrase, which offered 3 choices for the passphrase: short, all lowercase, and random.

Multiple emails were sent out to remind users of the approaching deadline. Five days before the deadline, 94% of passwords were unchanged. One day before the deadline, 29% were unchanged. A month after the deadline, with locking accounts of those whose passwords had not changed, 12% of passwords remained unchanged. A small number of these people had already left the organization. Some of the remaining portion were people protesting, being unhappy their credentials were revoked for any reason, calling it a basic user right. On concluding this event, most people ended up using randomly generated password. Finally, a

non-negligible fraction of the users with unchanged passwords never logged in. Conclusion: Scientists cared much less about privacy and more about their “right to access”, equating having credentials to being a member of LIGO.

A Case Study on Implementing Crowdsourced Threat Intel and Active Response -

Charley Kneifel and Richard Biever

An approach to supplement vendor supplied threat intelligence with organization generated or crowdsourced threat intelligence was tried. Threat intelligence is not just data, it also includes information discovered through analysis. In constructing an infrastructure, Duke went through many steps, including creating new firewalls and network flow collectors, black hole routing, and DNS query analysis. Virtualizing honeypots and sharing data were added in 2018. This list of infrastructure defenses is a good example of defense-in-depth approach. To add sharing intelligence, the program STINGAR was used, which makes use of network sensors and network metadata system logs files to identify and block attackers as well as compromised machines and accounts. For example, honeypots in the science DMZ at Duke are hit with 3000 events a day, with only 200 unique IP addresses. The primary activity is network scanning and SSH and web authentication brute force attempts. This intelligence is shared with other groups.

Evidence Based Cybersecurity - Grayson Harbour

Evidence based cybersecurity is an approach to cybersecurity practice that prioritizes the use of rigorous research products, real world facts, and direct observation to drive decision-making. It is an attempt to address the lack of evidentiary support in many cybersecurity standards and compliance regimes, and the black box approach to control set production. “Evidence based” is derived from medical context; there are parallels between medicine and security, including the ability to choose the best research and the distinguishing features of clinical expertise. Future sources of evidence could be improved by including central databases, increasing auditability, publishing research with accessibility in mind, and treating cybersecurity as a public health issue.

Security and Assurance for Research Identities - Panel

Moderator: *Jim Basney*

Panelists: *Laura Paglione, Steve Tuecke and Romain Wartel*

The final panel of the summit explored the current state of identity management within research, as well as for systems to maintain identities (specifically ORCID), identity migration through Globus and finally the incentive to protect identities due to their value within black markets -- the latter which will require a form of federated incident response (IR). The key result from this panel echoed those from earlier presentations and panels, i.e., we as a

community need to develop a efficient process for vetting trust between federated security entities in order to improve trustworthy science within research and education.

4 Community Observations and Future Challenges

The 2018 summit not only progressed on recommendations and opportunities exposed in past summits, but also in identifying new, key insights the community touched on this year. In Section 4.1 “Findings”, we lay out factual information collected from the current year’s summit. This distilled information is then used in Section 4.2 “Observations” to suggest important work that the community should continue to investigate as future challenges.

4.1 Findings

Findings are factual determinations made as a result of the summit. Findings serve to provide insight into the cybersecurity landscape of the NSF Community, and help form the basis for observation, i.e., future challenges.

4.1.1 Trust Relationships

Current processes for establishing and quantifying trust relationships, vetting new members and sharing information between community members is intractable. Thus, members could benefit from re-evaluating the current processes and seeking alternative, more tractable solutions.

4.1.2 Human factors

The human factor in security events is perpetually overlooked. Although user education and awareness has always been a critical component of a strong security program, based on reported experiences human error continues to be a major factor in security events. The community needs to better understand the interaction between humans and security, and to explore the possibility of users taking a bigger role in security solutions, not simply being educated on the risks that their actions may incur.

4.1.3 Positive Cybersecurity Metrics

Metrics used in demonstrating the effectiveness of security controls almost universally speak in negatives, e.g., some percentage of hosts compromised. Thus, even if a mitigation technique is functioning as expected, there is still a negative connotation to the metric that relates it to malicious or adverse events. The community as a whole should learn to market cybersecurity solutions with positive metrics.

4.1.4 Summit Impact

There was agreement regarding the value the summit and its related cybersecurity materials provide to the community. The lessons learned talks showcased the need for stronger trust relationships, while presentations like the one given by Charley Kneifel and Richard Biever exposed community members to the state-of-the-art in cybersecurity. Similarly, summit trainings were extremely popular, building on the growth from previous years. A clear majority of the attendees identified themselves as experiencing, or interested in, the topics and material presented, and thus, being directly impacted by the summit.

4.2 Observations

As with past summits (see Appendix A), accumulated findings and key insights are examined at the conclusion of the summit, and if warranted, are expressed as challenges in order to direct future efforts. Challenges are intended to offer exploratory topics to the broader NSF community, and should serve as a foundation for challenges or even recommendations for future summits.

4.2.1 Establishing Trust Relationships: Trust communities are essential for sharing sensitive information between those tasked with securing cyberinfrastructure. NSF cyberinfrastructure members can benefit from stronger trust communities in order to mitigate against the current distributed threat landscape. This requires re-evaluating how current trust relationships are established, as well as how information is shared between community members, which in itself, will require the community to overcome its fear of security breaches.

Based on the importance of trust communities, we reach our first observation:

Observation 1: NSF cyberinfrastructure projects need to develop a more tractable method in establishing trust relationships, as well as sharing information over established channels. This may require reevaluating the tradeoffs of sharing information regarding experienced breaches.

4.2.2 Mitigating Human Error: User education and awareness has always been a critical component of a strong security program. It is essential for users to be cognizant of the risks incurred from their use of a project's cyberinfrastructure. However, based on reported experiences at the summit, the human factor continues to be a major factor in security events. In short, the community needs to better understand the interactions between humans and security processes in place to protect the cyberinfrastructure, and then re-evaluate how user awareness is disseminated and what is included within the disseminated information. Moreover, the community should explore the possibility of users taking a bigger role in security solutions, as opposed to being content with simply educating the user on the potential risks

that their actions may incur.

Observation 2: NSF cyberinfrastructure projects need to examine how and what information is presented to the user during awareness and education, as well as to see if there are better avenues or opportunities to encourage the user to be more involved in the security process.

4.2.3 Promoting Positive Security Metrics: The success of security controls applied to CI are typically quantified through metrics that highlight the malicious nature of the adversary, e.g., some percentage of hosts compromised. This, unfortunately, results in the situation that even if a mitigation technique is functioning as expected, there is still a negative connotation to the metric that relates it to malicious or adverse events. However, other CI enhancements, e.g., additional RAM, promote the increased productivity yielded by the user of the CI. Thus, the community needs to pursue a rhetoric that markets cybersecurity solutions with positive metrics.

Observation 3: Cybersecurity needs positive or proactive metrics, as opposed to presenting negative events and the risks associated with the lack of cybersecurity. Historically, the efficacy of security mechanisms has been presented in terms of attacks thwarted, e.g., the firewall has blocked n malicious packets, rather than in terms of positive productivity, e.g., n users accessed the database without complications.

5 The Organizing and Program Committees

The 2018 summit was organized and hosted by Trusted CI, the NSF Cybersecurity Center of Excellence. Five members of that project (Ryan Kiser, Jim Marsteller, Mark Krenz, Austin Mitts, and Diana Borecky) along with Leslee Cooper, the Administrative Director for the Indiana University Center for Applied Cybersecurity Research, served as the organizing committee. We recruited a Program Committee (PC) comprising key leaders from NSF CI projects and the broader community. The PC was responsible for setting the agenda and inviting speakers, evaluating and selecting training, talks and panels, extending invitations to expert presenters, participating actively in the event itself, and laying the framework for successful post-summit evaluation and community support. Jim Marsteller served as chair of the PC, a role he has held in prior summits. The PC held 15 meetings by conference call beginning February 28, 2018 and ending August 8, 2018. It conferred electronically both prior to and following this time period.

The 2018 PC members were:

- **Steve Barnett**, Senior System Administrator for the IceCube Neutrino Observatory.
- **Anthony (Tony) Baylis**, Assistant Department Manager for the Computing Applications and Research Department in the Computation Directorate at Lawrence Livermore National Laboratory.
- **Michael Corn**, CISO of the University of California at San Diego where he manages the Security Office as well as the Identity and Access Management.
- **Dr. David Halstead**, CIO for the National Radio Astronomy Observatory. His responsibilities are divided between Data Management for the Observatory's HPC infrastructure in support of the national radio telescopes, and the general IT support for NRAO's 500+ employees.
- **Susan Ramsey**, Risk Assessor and Security Engineer at the National Center for Atmospheric Research.
- **Victoria Strodden**, Associate Professor, School of Information Sciences at the University of Illinois Urbana-Champaign.
- **Florence Hudson**, Special Advisor, Trusted CI, NSF Cybersecurity Center of Excellence at Indiana University.

6 The Call for Participation

The PC issued a call for participation (CFP) to the community requesting submissions in the form of: (a) white papers one to five pages in length, focused on unmet cybersecurity challenges, lessons learned, and/or significant successes; (b) one to two page abstracts for proposed half-day or full-day training; (c) one to two page abstracts for proposed table talk sessions; or (d) student applications.⁴ The PC also requested one to five page length nominations for outstanding leadership in the cyberinfrastructure and cybersecurity field for the Community Leadership Recognition Program.

The CFP continued a process started in 2014, designed to elicit a greater degree of community participation in developing the agenda, executing the summit, and increasing our ability to identify summit findings that represent the concerns, successes, and aspirations of our community. The 2014 CFP process was expanded in 2015, and a "Tips for Building CFP

⁴ The full Call For Participation (CFP), as well as the full summit program can be found at <https://trustedci.org/2018-nsf-cybersecurity-summit/>.

Responses” was provided to guide and encourage respondents and additional content formats were considered. The 2018 CFP process proved a success, and drove a great deal of the resultant program, including a mix of 14 plenary submissions, 2 table talks, 8 training sessions, including a full day workshop as well as a keynotes from the community at large, and presentations from key leaders from within the NSF community. For the third year in the row, we had a strong response in CPF proposals, again exceeding our capacity to accommodate all of the submissions.

7 Summary of Attendees

Summit registration was open to all interested individuals, a change made in 2016. This was done to avoid being insular, and to maintain and develop new relationships, and encourage infusion of additional perspectives. Registration was granted to all parties who requested to attend and were able to demonstrate a connection to the community. This year we added a \$200 registration fee to enable expanding the summit for the community. Our invitation list was based on the invitation list from the 2017 summit, and was updated to account for changes in the community, suggestions from NSF staff, and speakers to address specific topics of the summit. The invitation list included those with direct cybersecurity responsibilities in NSF Large Facilities and CI projects, NSF project principal investigators, and other key stakeholders and risk owners to help ensure that NSF cybersecurity evolves to address their needs.



Fig. 1 NSF Summit Attendees

One hundred seventeen (117) individuals registered for the summit. Ninety five attendees participated in the August 21 training sessions. Thirty six individuals - over a third of participants - participated in planning, spoke, provided training, co-authored a CFP submission, and/or led a lunch table talk. Six attendees were students. Twenty eight attendees work at Large Facilities. Seven attendees work at the NSF.

This year we were excited to welcome back WISE who held a full day workshop at the summit⁵ for a second year. WISE includes representative from many European E-Infrastructures including SURF, Hikhef, GÉANT, EGI, CERN, PRACE and EUDAT. The workshop featured US and international security experts collaborating on a variety of topics including collaboration between WISE and Trusted CI on best practices and policies, EU GDPR data privacy, and the formation of a new networking group on security in high throughput data transfers.

7.1 NSF Project Representation

Attendees were asked to provide the NSF project or other organization (NSF directorate in the case of NSF staff) with which they were associated including the NSF award number if applicable and their NSF Directorate. The following list contains a normalization of the provided

⁵<https://wise-community.org/2018/08/24/the-wise-community-makes-good-progress-while-usa-news-teams-are-gathered-outside/>

answers. 53 projects, including 21 large facilities (marked with “◆”), were represented at the summit by representatives of those projects. NSF directorates represented in some manner included: BIO/DBI, CISE/CNS, CISE/IIS, CISE/OAC, MPS/AST, MPS/DMR, MPS/PHY, EHR/DGE, EHR/DUE, ENG/CMMI, GEO/AGS, GEO/EAR, GEO/OCE.

We note some answers given represent NSF projects (e.g., “CC-IIE”) or other general areas of the NSF community (e.g., “Science Gateways”) which are not very precise. We will work on obtaining more precise specification of awards in future summits to improve our understanding of community representation.

- A Toroidal LHC Apparatus (ATLAS) Detector Operations and High Luminosity Upgrade Design ◆
- A Toroidal LHC Apparatus (ATLAS) Detector Phase I Upgrade ◆
- Accomplishment Based Renewal (ABR) to the award Flight-Worthy Condor: Enabling Scientific Discovery
- Atacama Large Millimeter Array (ALMA) ◆
- Advanced Technology Solar Telescope (ATST)
- Blue Waters
- Bridges: From Communities and Data to Workflows and Insight
- Center for Trustworthy Scientific Cyberinfrastructure (CTSC)
- CC-NIE Integration: OneOklahoma Friction Free Network
- CICI: Secure and Resilient Architecture: Creating Dynamic Superfacilities the SAFE Way
- CIF21 DIBBs: An Integrated System for Public/Private Access to Large-Scale, Confidential Social Science Data
- Collaborative Proposal: Capacity Building in Cybersecurity: Broadening Participation of Women In Cybersecurity through Women in Cybersecurity Conference & Professional Development
- Collaborative Research: CyberWorkshops: Resources and Strategies for Teaching Cybersecurity in Computer Science (CReST)
- Daniel K. Inouye Solar Telescope (DKIST)
- EAGER: Cybersecurity Transition To Practice (TTP) Acceleration
- EAGER: Designing the OSN Software Platform
- Extreme Science and Engineering Discovery Environment (XSEDE)
- Gateways to Discovery: Cyberinfrastructure for the Long Tail of Science
- GEMINI observatory ◆
- Geodesy Advancing Geosciences and Earthscope (GAGE Facility)
- Green Bank Observatory ◆
- HTCondor
- IceCube Neutrino Observatory ◆

- International Ocean Discovery Program (JOIDES Resolution) ♦
- International Ocean Discovery Program (Science Support Office) ♦
- IRNC-BackBone- TransPAC4 - Pragmatic Application-Driven International Networking
- IRNC: AMI: NetSage - An Open, Privacy-Aware, Network Measurement, Analysis, and Visualization Service
- IRNC: Backbone: NEAAR: Networks for European, American, and African Research
- Jetstream
- Laser Interferometer Gravitational-Wave Observatory (LIGO) ♦
- Large Hadron Collider ♦
- Large Synoptic Survey Telescope (LSST) ♦
- Long Baseline Observatory ♦
- National Center for Atmospheric Research (NCAR) ♦
- National High Magnetic Field Laboratory (NHMFL) ♦
- National Optical Astronomy Observatory (NOAO) ♦
- National Optical Astronomy Observatory (CTIO)
- National Radio Astronomy Observatory (NRAO) ♦
- National Solar Observatory (NSO) ♦
- Natural Hazards Engineering Research Infrastructure (NHERI) ♦
- Ocean Observatories Initiative (OOI) ♦
- Open Science Grid (OSG)
- Regional Class Research Vessel Program ♦
- SaTC: EDU: Collaborative: Enhancing Security Education through Transiting Research on Security in Emerging Network Technologies
- SAVI: Building a framework between the EU and the USA to harmonize data products relevant to global research infrastructures in the environmental field
- SecKnitKit (Security Knitting Kit): Integrating Security into Traditional Computer Science Courses
- SI2-SSI: Pegasus: Automating Compute and Data Intensive Science
- SS2-SSI: The Agave Platform: An Open Science-As-A-Service Cloud Platform for Reproducible Science
- TENNESSEE CYBERCORPS: A HYBRID PROGRAM IN CYBERSECURITY
- Very Large Array (VLA) ♦
- Wall of Wind (Florida International University) ♦
- WISE
- XSEDE 2.0

Note: while general participation from the community has grown over the years, participation from NSF program officers at the Cybersecurity Summit continued to drop lower this year with

7 NSF staff attending. This is down from 9 in 2017, 12 in 2016, and 18 in 2015.

7.2 Student Representation

In addition to professionals, the Summit included the participation of six students via a scholarship program. Students were encouraged to apply to the program but could also be nominated by a mentor or teacher. They were asked to provide a one-page letter describing their interest and any relevant experience with cybersecurity, emphasizing the benefit of attendance to the student and/or community.



Fig. 2 Student Summit Attendees
(Left to right: Emily Dillon, Sanchari Das, Grant Allard, Preston Ruff, Maggie Ahern, Leah Dorman)

The Program Committee reviewed all submissions with an interest in advancing diversity and inclusiveness, selecting six exceptional students: Emily Dillon, Master of Science student at Capella University; Sanchari Das, PhD student at Indiana University; Grant Allard, PhD student at Clemson University; Preston Ruff, Bachelor of Science student at New Mexico Institute of Mining and Technology; Maggie Ahern, Bachelor of Science student at Lehigh University; and

Leah Dorman, Bachelor of Science student at University of Maine Augusta.

The students were paired with mentors: volunteers from the program committee and Summit attendees, to encourage their participation during the Summit and beyond.

While at the Summit, students and mentors met for breakfasts and lunches, and attended the program committee dinner. In the opening remarks, Jim Marseller asked the students to introduce themselves and their areas of interest in cybersecurity. Students were also assigned the task of taking notes during the table talk sessions.

These small gestures allowed the students to ask any questions and do professional networking. This program has demonstrated tremendous success, and we have received positive feedback from both students and mentors.

A month after the Summit, we asked the students to share their thoughts on participating in the event. A few noteworthy quotes:

“The mentoring initiative associated with the student program is a superb educational tool that helped me put my experience in context and learn from one of the leaders of this field.” -- Grant Allard

“I am incredibly grateful that I was given this opportunity to learn more about this subject and meet new individuals passionate about cybersecurity.” -- Maggie Ahern

The full comments from the students are in Appendix E.

7.3 Inclusiveness

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. In 2014, we expressly addressed the topic with the PC, identifying two members to spearhead efforts (Baylis, Hassler). The group sought to encourage diverse participation via the invitees, speakers, panelists, and PC itself. Additionally, the CFP expressly gave priority to those students from groups underrepresented in the NSF information security workforce. We note that Baylis has specific experience in this area as chair of the Supercomputing Broader Engagement in 2008 and participated in that committee in 2009. In 2018 we instituted the “NSF Cybersecurity Summit Rules and Code of Conduct” to provide guidance on the type of behavior that is expected while in attendance at the conference.⁶ Deputy Office Director of the Office of Advanced Cyberinfrastructure (OAC) Amy Friedlander commended the adoption of this new

⁶ <https://trustedci.org/nsf-cybersecurity-summit-code-of-conduct>

policy in her opening remarks.

In order to gather ongoing baseline data related to this diversity effort, registrants had the option to provide their ethnicity/race and gender/sex. The aggregated responses to the those items follow. Voluntary responses to these questions show:

Table 1. Attendee self-reported ethnicity.

Ethnicity / Race	2018	2017	2016
Asian or Southeast Asian	8 (6.8%)	11 (8.4%)	8(8%)
Black or African American	1 (0.8%)	4 (3.1%)	3(3%)
Hispanic or Latino	1 (0.8%)	4 (3.1%)	3(3%)
Native Alaskan or American Indian	0 (0%)	1 (0.8%)	0
Multiracial	2 (1.7%)	4 (3.1%)	0
White or Caucasian	84 (71.2%)	79 (60.8%)	60(60%)
Other Ethnicity	1 (0.8%)	0 (0%)	0
Other (space provided)	0 (0%)	1 (0.8%)	0
Prefer not to answer	7 (5.9%)	10 (7.7%)	5(5%)
No Answer Provided	14 (11.9%)	16 (12.3%)	21(21%)

Table 2. Attendee self-reported gender.

Gender / Sex	2018	2017	2016
Female	18 (15.3%)	27 (20.8%)	16(16%)
Male	75 (63.6%)	77 (59.2%)	59(59%)
No Answer Provided	25 (21.2%)	26 (20%)	25(25%)

8 Attendee Evaluations

We sought attendee evaluations of the summit via two SurveyMonkey surveys. One survey gathered feedback specific to the summit’s plenary sessions, i.e., the Attendee Survey; the other requested feedback for those attending the August 21 training sessions (the Training Survey). The general and training survey results are appended to this report as Appendix F.

Overall, the summit survey responses were generally positive and extremely thoughtful. Fifty attendees (approximately 42% of all attendees) responded to the general “Attendee Survey.”⁷ Of the fifty responses, 98% rated the overall summit experience either very good or good, with

⁷ The organizers did not submit response, but the survey was open to all other participants.

one person rating it average. A sample comment from the question asking *How can we improve the summit experience in the future?*, follows: “Add an unconference segment, perhaps after the plenary sessions. Provide a 2-3 hr slot for sharing lessons learned. Adopt the rule that ‘what’s said in this room stays in this room.’ Have a period at the end of the slot to agree on what may be said outside of the room, ie, what can be published about lessons learned.” Similarly, a thoughtful response to the question *Were there any aspects of the summit you found particularly useful or important?*, was “A convergence of thinking on how to approach cybersecurity and compliance (without fear of breaches), an extension of C, I, A to E, T, R, and Breach report.”

The Training Day preceding this year’s summit offered eight training sessions, including: the WISE (Wise Information Security for collaborating E-infrastructures) Workshop; Industrial Control System Security - Existing Infrastructure and New Designs; Setting up a compliance program for CUI; Automated Assessment Tools - Theory & Practice; Developing Cybersecurity Programs for NSF Projects; Software Engineering Guide for NSF Science; Compliance 101: HIPAA, FISMA, NIST 800-171 and GDPR; and Security Log Analysis Training. As with the general survey, most respondents to the training survey gave positive feedback, with the responses to the question asking if they would participate at future summit training sessions overwhelmingly positive with 36 of the 38 survey participants answer “yes.”

Additionally, responses to tutorial-specific surveys were also positive and included constructive feedback as well as ideas for future training offerings. When asked *What training topics would you like to see covered at future summits?*, 16 participants answered with vastly different requests, including: best practices, incident response, business continuity, disaster recovery planning, surveys on site implementations of compliance, IPv6 security, information classification, asset inventory methods, critical infrastructure protection for NSF specific facilities (nuclear, arctic, etc.), transition to practice, strategic cybersecurity planning, IDS/IPS implementation and tuning, internal auditing, high speed/large volume security, vulnerability risk assessment, patching approaches, web application firewalls, MFA options, approaches and tools for web application security assessments, overview by NSF of which projects they are funding related to cybersecurity grants and research, cloud security, IAM, demo of use of security tools in NSF projects, Big Data/Machine Learning introduction, and new risk management frameworks.

9 Conclusion

We relaxed the structure of the summit this year to encourage the participants to branch out,

pursuing topics most relevant to them. The result was pleasing, but simultaneously surprising, in that one of the primary insights the participants continued to converge on was “building trustworthy relationships” -- something not on our agenda. The fact that the community steered the summit to something they deemed relevant bodes well for future summits and continuing to encourage participants to delve into uncharted topics. Moreover, it is encouraging that the community participation and response to call for proposals remained strong. We thank the community members who helped the summit achieve its goals. In particular, we thank those who served on the program committee for their effort and devotion to the summit.

We are excited for next year’s summit and for the opportunity to confront new cybersecurity challenges in our unique and collaborative environment. This opportunity will require that we, the program committee and the community, continue to be vigilant in identifying new and relevant areas for discussion at next year’s summit. We will continue to evolve and improve upon the summit to adapt to the community’s changing needs, e.g., adjusting our registration model to expand participation by the NSF and broader communities.

Finally, we thank the NSF for funding the summits and providing presentations.

Appendix A: Recommendations From Past Summits

This appendix serves as a compendium for all recommendations made in past summit reports. The exact role of these “recommendations” has shifted over time, with some recommendations being directly carried over from year-to-year, while others rebranded as “Opportunities.” Despite this changing usage, this appendix should provide a comprehensive perspective of the takeaways from past summits, and serves to inform recommendations made in this and future summit reports.

2017 Recommendations:

Note: In 2017, the number of recommendations were reduced in order to focus efforts.

Recommendation 1: NSF projects should have budgets for cybersecurity in the range of 3-12% of total IT budget. Projects with cybersecurity budgets below that range should carefully consider the appropriateness of their budget.

Recommendation 2: NSF projects should engage and incorporate stakeholders and senior leadership into the information security risk acceptance and risk management processes. This should include explicitly delineating responsibilities and accountability among the relevant actors.

Recommendation 3: NSF projects should look to a broader range of cybersecurity standards and frameworks when selecting what will provide the best fit for their mission.

Recommendation 4: NSF projects should continue to refine Risk-based approaches to help provide the most nuanced and applicable information to cybersecurity stakeholders, and may wish to draw from a broader range of sources, such as the AFCEA Economics of Cybersecurity and the Information Security Practice Principles.

2016 Recommendations:

Note: the 2016 Summit Report carried over the Recommendations from the 2015 Report.

Recommendation 1: The NSF CI and Large Facility community should develop a broadly applicable strategy for information security budgets, including how, why, and where it does what it does in terms of spending.

Recommendation 2: The NSF CI and Large Facility community should support research on metrics that indicate whether spending on information security is sufficient and appropriately

balanced with a project's science mission.

Recommendation 3: The NSF CI and Large Facility community should develop a common understanding among all stakeholders of how accountability, risk responsibility, and risk acceptance practices are most efficiently and appropriately distributed among project leadership, project personnel, and other stakeholders.

Recommendation 4: The NSF CI and Large Facility community should determine its software assurance, quality, and supply chain requirements.

Recommendation 5: Utilizing a consensus process that includes all stakeholders, the NSF CI and Large Facility community should adopt a common, broadly applicable framework for information security.

Recommendation 6: The NSF CI and Large Facility community should continue to implement, refine, and evaluate risk-based approaches to cybersecurity that leverage established best practices as much as possible, while also addressing the community's particular needs around unique scientific instruments, data, openness, multi-organizational relationships, mission assurance, resilience, and project lifespans.

Recommendation 7: The NSF CI and Large Facility community should find more ongoing ways of collaboratively developing and maintaining cybersecurity programs, such as sharing materials, services, practices, lessons learned, and collaborative/peer reviews.

Recommendation 8: The NSF CI and Large Facility community should continue to develop and disseminate best practices for identity and access management to support research.

Opportunity 1: The NSF CI and Large Facility community should explore how it can support, participate in, and directly benefit from basic and applied cybersecurity research like that funded via NSF's Secure and Trustworthy Cyberspace (SaTC) and Risk and Resilience solicitations.

Opportunity 2: The NSF CI and Large Facility community should closely follow, participate in, evaluate, and validate the NSF Cybersecurity Center of Excellence's community threat model development effort, including determining whether insights into threat actors and threat events positively impact the efficiency and effectiveness of our cybersecurity programs and risk management processes.

Opportunity 3: The NSF CI and Large Facility community should explore collaboration with, and even drive change in, existing cross-organizational mechanisms (e.g., REN-ISAC, EDUCAUSE, Internet2) where information sharing can efficiently and effectively help the community gain a

defensive advantage.

Opportunity 4: The NSF CI and Large Facility community should determine when and how privacy intersects with NSF CI cybersecurity efforts in terms of (i) legal and regulatory requirements; (ii) our community's norms, values, and stakeholder relationships; and (iii) being a barrier to and/or enabler of science

2015 Recommendations:

Recommendation 1: The NSF CI and Large Facility community should develop a broadly applicable strategy for information security budgets, including how, why, and where it does what it does in terms of spending

Recommendation 2: The NSF CI and Large Facility community should support research on metrics that indicate whether spending on information security is sufficient and appropriately balanced with a project's science mission.

Recommendation 3: The NSF CI and Large Facility community should develop a common understanding among all stakeholders of how accountability, risk responsibility, and risk Report of the 2015 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure 16 acceptance practices are most efficiently and appropriately distributed among project leadership, project personnel, and other stakeholders.

Recommendation 4: The NSF CI and Large Facility community should determine its software assurance, quality, and supply chain requirements.

Recommendation 5: Utilizing a consensus process that includes all stakeholders, the NSF CI and Large Facility community should adopt a common, broadly applicable framework for information security.

Recommendation 6: The NSF CI and Large Facility community should continue to implement, refine, and evaluate risk-based approaches to cybersecurity that leverage established best practices as much as possible, while also addressing the community's particular needs around unique scientific instruments, data, openness, multi-organizational relationships, mission assurance, resilience, and project lifespans

Recommendation 7: The NSF CI and Large Facility community should find more ongoing ways of collaboratively developing and maintaining cybersecurity programs, such as sharing materials, services, practices, lessons learned, and collaborative/peer reviews.

Recommendation 8: The NSF CI and Large Facility community should continue to develop and disseminate best practices for identity and access management to support research.

Recommendation 9: The NSF CI and Large Facility community should determine when and how privacy intersects with NSF CI cybersecurity efforts in terms of (i) legal and regulatory requirements; (ii) our community's norms, values, and stakeholder relationships; and (iii) being a barrier to and/or enabler of science.

Recommendation 10: The NSF CI and Large Facility community should explore how it can support, participate in, and directly benefit from basic and applied cybersecurity research like that funded via NSF's Secure and Trustworthy Cyberspace (SaTC) and Risk and Resilience solicitations.

Recommendation 11: The NSF CI and Large Facility community should closely follow, participate in, evaluate, and validate the NSF Cybersecurity Center of Excellence's community threat model development effort, including determining whether insights into threat actors and threat events positively impact the efficiency and effectiveness of our cybersecurity programs and risk management processes.

Recommendation 12: The NSF CI and Large Facility community should explore collaboration with, and even drive change in, existing cross-organizational mechanisms (e.g., REN-ISAC, EDUCAUSE, Internet2) where information sharing can efficiently and effectively help the community gain a defensive advantage.

2014 Recommendations:

Recommendation 1: The NSF CI and Large Facility community should define its own best practices for cybersecurity rather than anticipating detailed direction from NSF. Clearly setting our own standards will help protect us from compliance directives not as well-suited to our community.

Recommendation 2: The NSF CI and Large Facility community should implement a risk-based approach to cybersecurity that leverages broader best practices as much as possible, while addressing and balancing the community's particular needs around unique scientific instruments, data, openness, multi-organizational relationships, and project lifespans.

Recommendation 3: The NSF CI and Large Facility community should identify and share best practices for how to successfully integrate security throughout and across project organizations.

Recommendation 4: The NSF CI and Large Facility community should develop a common understanding of how risk responsibility and acceptance practices are most efficiently and appropriately distributed among project personnel and stakeholders.

Recommendation 5: The NSF CI and Large Facility community should explore ways of collaboratively developing and maintaining cybersecurity programs, such as sharing materials, services, policies, practices, lessons learned, and collaborative/peer reviews.

Recommendation 6: The NSF CI and Large Facility community should continue to find ways of sharing real-time data in order to foster continuity of expertise and gain as much of an advantage as possible in defending ourselves. Existing cross-organizational mechanisms (e.g., REN-ISAC, EDUCAUSE, Internet2) should be evaluated in terms of how they could be leveraged.

Recommendation 7: We recommend the NSF CI and Large Facility community undertake or support a research effort to increase understanding and communicate that knowledge or know-how for each of the following open questions:

D. What is the threat profile for our community, and can insights into threat actors and their motivations positively impact the efficiency and effectiveness of our cybersecurity programs and risk management processes?

E. When and how does privacy intersect with NSF CI cybersecurity efforts in terms of (i) legal and regulatory requirements; (ii) our community's norms, values, and stakeholder relationships; and (iii) being a barrier to and/or enabler of science?

F. How do we include and meaningfully address software assurance, quality, or supply chain in the context of the project cybersecurity programs, and the summit itself?

2013 Recommendations:

Recommendation 1: The community should identify a means to organize future summits.

Recommendation 2: Future summits should continue to include NSF project principal investigators, other key stakeholders and risk owners to ensure that NSF cybersecurity evolves to address their needs.

Recommendation 3: Future program committees should consider more time and opportunities (e.g., increased seating) for tutorials, hands-on activities, and organized discussion.

Recommendation 4: Future program committees should take on gender, age, and racial/ethnic diversity in the community and the summit attendance as a strategic imperative for future

summits.

Recommendation 5: The community should consider the relationship between large facilities and smaller cyberinfrastructure projects, and their potential synergies around cybersecurity, as well as how (and if) the summit can effectively address both.

Recommendation 6: The community needs to develop a better understanding of the expectations for their cybersecurity programs and how to meet those expectations.

Appendix B: Descriptions of Workshops and Training Sessions

Tuesday, August 21st featured a full day of focused workshops and training, available to all registrants. All but the WISE Workshop and Federated Identity Management for Research Organizations were half-day offerings.

Concurrent Morning Sessions

WISE Workshop (Full Day)

Instructors: WISE Community

About WISE: The WISE (Wise Information Security for collaborating E-infrastructures) community was born as the result of a first workshop in October 2015. It was agreed then that collaboration and trust is the key to successful information security in the world of federated digital infrastructures for research. WISE is an international community with participants spanning North America, Europe, Asia and Australia.

Full agenda: <https://wiki.geant.org/display/WISE/WISE+@+NSF+CyberSecurity+Summit+2018>

WISE provides a trusted global environment where security experts from general and research domain-specific Infrastructures can share information on topics such as risk management, experiences about certification processes and threat intelligence. With participants from e-Infrastructures such as EGI, EUDAT, GEANT, EOSC-hub, PRACE, XSEDE, OSG, NRENs and more, the main aim of WISE is to promote best practice in Information Security by developing trust frameworks, template policies and guidelines for e-Infrastructures.

The actual work of WISE is performed in focussed working groups, each tackling different aspects of collaborative security and trust. This year we have 3 new working groups which are currently starting their work. While many of the working group activities are performed by conference calls and e-mail, experience has shown that we can make very good progress by holding face to face WISE events. These events, which typically attract between 20 and 40 participants, are held at least twice a year. We have already met once in 2018 in Europe (Abingdon, UK, February), and we propose that this WISE training/workshop at the NSF Cybersecurity summit would be an excellent way of fulfilling the desire for a second event in North America.

We propose a full-day WISE Community Security Training event at the 2018 NSF Summit. We were very happy to be able to run such an event in 2017 and propose to build on what was then a very successful day. The activities/working groups we propose for possible inclusion in the 2018 one-day

WISE are:

- Security challenges for high-throughput data transfers
- Operational Security threat intelligence and communication between Security Operations Centres (SOCs), e.g. use of MISP etc.
- Security for Collaborating Infrastructures
 - A training section to teach Infrastructures how to self-assess against the Trust Framework (V2)
 - Including use of a Policy Development Kit aimed at meeting the SCI needs
- We would also like to compare our policy kit with other such activities (Trusted CI for example) and see what we can learn from each other
- How to meet the requirements of EU GDPR in terms of policies and procedures for our e-Infrastructures

We will not have time to include all of these and the final choice will depend on which individuals are successful in achieving funding to attend, but we propose to cover 3 of the above topics during the day.

Target Audience for the training: We would invite security representatives from E-Infrastructures and Large-Scale NSF facilities to participate. This includes operational security individuals and policy makers. Some of the topics would be training sessions with hands-on exercises while others would be management/planning/brainstorming sessions, to assist the working groups in the production of new template policies and best-practice documents.

Industrial Control System Security - Existing Infrastructure and New Designs

Instructor: Phil Salkie (Jenariah Industrial Automation)

Summary: This breakout session provides an overview of “Industrial ControlSystem” (ICS) and “Supervisory Control and Data Acquisition”(SCADA) equipment, provides a process for managing the security of existing systems in your facility, and discusses the implications of designing in security when new equipment is specified for purchase.

Details: Most large scientific and data processing facilities have a variety of ICS and SCADA systems installed throughout the plant, controlling building systems such as Heating/Ventilation/Air Conditioning, Emergency Power Generation, and Building Security. Often, these systems are poorly understood, do not have data backup/restore plans, and/or fall in a “gray area” domain between

Facilities and IT departments. The harm that can be caused to a facility by an ICS/SCADA outage may be orders of magnitude larger than the cost of the entire system, or the budget allocated to securing that system.

In this breakout session, we will become familiar with various forms of legacy and modern ICS and SCADA systems, and discuss the security implications presented by network intrusions by “bad actors” as well as the issues presented by equipment which may have no operational backup, no data backups, and no on-site ability to reload or restore a system which requires replacement or even general maintenance. We will discuss the necessary steps for Management to determine what ICS systems are present, what will be required to protect them properly, and the order to take those mitigations. When systems are slated to be replaced, it is critical for IT to take a role in the specification and design phase in order to ensure that systems are implemented in a way which does not simply make the Design Engineer’s job easiest. Security and Ease-Of-Use face much the same trade-off battle in the ICS/SCADA space as they do in the consumer/user space, but “Designing for Security” in ICS/SCADA is all but unknown. We will look at different methods of securing ICS networks, including compartmentation, firewalling, least privilege, and minimization of control surface - all things which are more work up front, and will likely not be put into a system unless they are specified by someone who has an understanding of computer security issues.

Setting up a compliance program for CUI

Instructor: Erik Deumens (University of Florida)

Goals:

1. Provide the context and the background for compliance requirements, including the complete stack from physical security, to training and business processes, to institutional buy-in from the university administration.
2. Clarify the difference between compliance for federal agencies, and other organizations, universities in particular.
3. The NIST guidelines for the Risk Management Framework (RMF) call for customization. Participants will be given information and then will be guided to design and plan a compliance program that suits their university, with its specific mission and budget, its specific political and regulatory context, and its administrative culture and climate.

Automated Assessment Tools - Theory & Practice

Instructors: Barton P. Miller and Elisa Heymann (University of Wisconsin)

This tutorial starts by teaching about a critical class of vulnerabilities, the injection; then follows with a description of software assessment tools that can identify such vulnerabilities in your code; and last, provides an opportunity to get hands-on experience in using these tools to identify and mitigate the vulnerabilities.

Injection attacks are always in the top 10 attacks that are commonly exploited and that have serious consequences. Notably, these attacks affect programs written in almost any language. In this tutorial we will present examples of code injection attacks and SQL injection attacks.

Then we will introduce different types of assessment tools, describe how they work, their output and their limitations. We will talk about control flow and data flow analyses, as they are foundational techniques used by many tools to determine if certain code is safe or not.

The next section of the tutorial explain how to use different commercial and open source tools for C/C++ and Java, and how to process the tools' output. We will use simple test applications extracted from the NIST/NSA Juliet test suite, where each of these applications contain code with the specific weaknesses and a version of the same code with the weakness fixed.

Then we will move on to the hands-on section of this tutorial. The students will use the Software Assurance Marketplace-SWAMP (<https://continuousassurance.org/>), an open facility that allows users to scan their software with different tools without the burden of dealing with tool acquisition, installation, and configuration. Through the SWAMP, users can access both commercial and open source software assessment tools. By using the SWAMP, the students will be able to identify problems in the given source code, modify the code, compile it, and submit it to the SWAMP for another assessment.

Developing Cybersecurity Programs for NSF Projects

Instructors: Kay Avila, Bob Cowles and Craig Jackson

This session will be based on an upcoming restructuring of the cybersecurity planning guide developed several years ago. The original guide was developed to address the information security requirements outlined in NSF cooperative agreements, but both the cybersecurity field and our understanding have evolved. The new version of the guide will be structured around the four pillars of cybersecurity as developed for the upcoming version of the Large Facilities Manual. However, the new guide should also be usable by the thousands of smaller NSF projects in determining their cybersecurity needs. This session will be appropriate both for attendees of last year's training of the

same name, as well as newcomers. Though there will be some overlap, we hope to use the updated presentation as an opportunity to explore areas in greater depth based on participants' needs.

The four pillars of cybersecurity:

- Mission alignment (hardware/software inventory and understanding mission-critical processes)
- Governance (policies and procedures, project leadership, risk management and acceptance, program evaluation)
- Resources (budget, personnel, 3rd party services, lifecycle considerations)
- Controls (baseline controls and specialized/alternative controls)

While this session will be instructional in nature, it is also intended to be an interactive session to seek constructive feedback from attendees as we improve the guide. There will be significant opportunities for discussion and Q&A.

Concurrent Afternoon Sessions

WISE Workshop (continued)

See Full Description Above.

Software Engineering Guide for NSF Science

Instructors: Susan Sons

Creating secure software is not simply a matter of coding each line better: it is a confluence of software engineering practice, tooling, and architecture *with* line-level secure coding practice. TrustedCI, the NSF Cybersecurity Center for Excellence, has been working on materials to help science projects which produce software, as well as scientific cyberinfrastructure projects, understand which engineering practices can give them the best return in software security for their effort, without hindering the science mission. An early draft of that material is now available, and this training will give those responsible for software in the NSF ecosystem the opportunity to work with it first. This half-day workshop will walk participants through the new Software Engineering Guide for NSF Science, using it as a basis to choose the software engineering practices that best enable the development of secure and robust software. The program will be primarily lecture, with a couple of short exercises interspersed.

Participants will learn to:

- Gauge the software engineering and security needs of a particular software development project.
- Select tools and processes appropriate to a project's security and reliability needs.

- Effectively guide user expectations surrounding security of the software.
- Handle vulnerability remediation.
- Use tooling and smart architecture to make the software development process itself easier and more reliable, not only increasing security, but reducing the costs of security and development in general.

Compliance 101: HIPAA, FISMA, NIST 800-171 and GDPR

Instructors: Anurag Shankar (Indiana University/CACR), Susan Ramsey (NCAR) and Scott Russell (Indiana University/CACR)

The regulatory burden flowing downstream from the funding agencies is growing ever stronger as a worsening cyber climate forces the government to introduce new privacy and security regulations in response. Ignorance is no longer an option for R&D organizations, including those that lack the necessary expertise and resources to acquire it. This training session is designed especially for them and others newly initiated but is likely to be useful generally. It demystifies HIPAA, FISMA, and NIST 800-171, US regulations that affect research, and GDPR, the new EU privacy regulation. It also offers guidance on ways to tackle the various compliance regimes through practical risk management.

Topics Covered:

- HIPAA, FISMA, and CUI Requirements (NIST 800-171). An introduction to the regulations, including scope, data types covered, and common misperceptions.
- GDPR. The new EU privacy regulation requiring data controllers and processors worldwide to protect the privacy of data for subjects in the EU.
- The NIST Risk Management Framework and NIST 800-53. A dive into cybersecurity standards.
- Managing Risk.
- Effective risk management by leveraging standards and practical tools.

Security Log Analysis Training

Instructor: Mark Krenz (Indiana University/Trusted CI)

The goal of security log analysis is to more efficiently leverage log collection in order to identify threats and anomalies in your organization. This half-day training will help you tie together various log and data sources to provide a more rounded, coherent picture of a potential security event. It will also help you understand log analysis as a life cycle (collection, event management, analysis, response) that continues to become more efficient over time. Interactive demonstrations will cover both automated and manual analysis using multiple log sources, with examples from real security

incidents.

Appendix C: Summit Agenda

2018 NSF Cybersecurity Summit Agenda

Tuesday August 21st - Thursday August 23rd, 2018

August 21st- Training Day

8:00am Registration and Continental Breakfast

9:00am Morning and All Day Training Sessions Begin

- WISE Workshop
- Industrial Control System Security - Existing Infrastructure and New Designs
- Setting up a compliance program for CUI
- Automated Assessment Tools – Theory & Practice
- Developing Cybersecurity Programs for NSF Projects

10:30am ***Coffee Break***

11:00am Training Sessions Resume

1:00pm ***Lunch provided***

2:00pm Afternoon Training Sessions Begin and All Day Training Sessions Resume

- WISE Workshop
- Software Engineering Guide for NSF Science
- Compliance 101: HIPAA, FISMA, NIST 800-171 and GDPR
- Security Log Analysis Training

4:00pm ***Coffee Break***

4:30pm Training Sessions Resume

6:00pm Sessions End

Evening: ***Dinner on your own***

August 22nd- Plenary Day 1

8:00am Sign-In and Continental Breakfast

- 9:00am Welcome and NSF Address (Jim Marsteller / Amy Friedlander)
- 9:30am Keynote: Von Welch - **“Five Years Backwards and Forwards”**
- 10:30am **Coffee Break (Meet a Student)**
- 11:00pm Involving Students in Cybersecurity for CI (Jeremy Straub)
- 11:30am Security Best Practices for Academic Cloud Service Providers (Rion Dooley, Richard Knepper, Mike Lowe)
- 12:30pm Group Photo, Lunch (**Lunch provided**) and Table Talks:
- Cybersecurity Research Transition To Practice (TTP): Needs, Solutions and US-EU Collaboration
 - Cybercrime book discussion
 - Industrial Control Systems/SCADA Security
- 2:00pm Silent Librarian (Kim Milford, Brett Zupan)
- 2:30pm Responding to advanced threats as a global community (Romain Wartel)
- 3:00pm XSEDE Lessons Learned (Adam Slagell)
- 4:00pm **Coffee Break**
- 4:30pm Incident Response Communications (Susan Ramsey, Ashwin Jacob Mathew, Dr. Daniel Massey)
- 5:30pm Open Discussion / Summary of the Day’s Findings (Jim Marsteller, Von Welch)
- 6:00pm Adjourn
- 6:30pm Social @ San Antonio Bar and Grill (200 Swamp Fox Rd, Alexandria, VA)
-

August 23rd - Plenary Day 2

- 8:00am Sign-In and Continental Breakfast
- 9:00am Password Adventures for a VO (Warren Anderson)
- 9:30am A case study on implementing crowdsourced threat intel and active response (Charley

Kneifel, Richard Biever)

10:00am Evidence Based Cybersecurity (Grayson Harbour)

10:30am ***Coffee Break***

11:00am Security and Assurance for Research Identities (Jim Basney, Laura Paglione, Steve Tuecke, Romain Wartel)

12:00pm Open Discussion / Summary of Summit Findings (Jim Marsteller, Von Welch)

12:30pm Adjourn

Appendix D: Bios for Speakers, Program Committee, and Organizers

Bios for Speakers, Authors, Program Committee Members, Organizers, and Student Awardees

In alphabetical order by surname

Maggie Ahern is a Junior at Lehigh University studying Computer Science and Engineering. Maggie is on the executive board of her university's Society of Women Engineers and has hosted STEM workshops and served as a counselor at STEM camps for young girls.

Grant A. Allard is pursuing his doctorate in Policy Studies at Clemson University. Allard's research agenda focuses on how science and technology policy and national politics affect the capacities of universities, governments, and industry to translate scientific research into new technologies such as cyberinfrastructure. Allard's research is transdisciplinary in scope using theory and research methods from policy studies, political science, economics, information science, and sociology.

Allard is interested in cybersecurity because of its vital role in maintaining the integrity of scientific cyberinfrastructure from both policy and technology transfer perspectives. From a policy perspective, it is important to understand how to integrate cyber security into scientific cyberinfrastructure projects without negatively affecting the scientific research process. Many scientific cyberinfrastructure projects are governmentally funded as extramural research meaning it is important to understand the decisions of governments related to promoting cybersecurity. From a technology transfer perspective, it is important to understand how to promote cybersecurity during the process of transferring scientific cyberinfrastructure from the "safer" environment of the laboratory to the "less safe" commercial or government environment.

Warren Anderson has a Ph.D. in theoretical physics from the University of Alberta and is the co-author of "Gravitational Wave Physics and Astronomy." He has been a member of the LIGO Scientific Collaboration for the last 20 years, where he has gradually transitioned from physics research to managing computational infrastructure. He has been the lead of the LIGO Identity and Access Management team since 2008 and a member of the LIGO Scientific Collaboration Security Committee since 2012. He has chaired or been a member of several InCommon committees and is currently a member of the the InCommon Community Architecture Committee for Trust and Identity.

Kay Avila (kayavila@illinois.edu) is a senior security engineer at the National Center for

Supercomputing Applications (NCSA) at the University of Illinois in Urbana-Champaign, where she works on Trusted CI and the Large Synoptic Survey Telescope (LSST) projects. Since joining Trusted CI in 2017, she has been involved with several engagements focused on developing and assessing security programs. Prior to this, she held positions in network security at a Fortune 500 insurance company and in higher education. Kay studied computer science and biology at the University of Northern Iowa.

Tom Barton is Sr. Consultant for Cyber Security & Data Privacy at the University of Chicago and a consultant to Internet2. Previously he was Senior Director and Chief Information Security Officer at U Chicago, and had earlier assignments as Director of IT Infrastructure and Director of Network Services at the University of Memphis, where he was a member of the mathematics faculty before turning to administration. He's a member of the Advisory Committee for Trusted CI, the NSF Cybersecurity Center of Excellence, Internet2's Community Architecture Committee for Trust and Identity (CACTI), the TIER Community Investors Council, the REFEDS Steering Committee, chaired the TIER Ad Hoc Advisory committee obsoleted by CACTI, and for many years led the Internet2 Grouper project.

Dr. Jim Basney is a senior research scientist in the cybersecurity group at the National Center for Supercomputing Applications at the University of Illinois at Urbana-Champaign. Jim's area of expertise is identity management for scientific collaborations. He is PI of the CILogon and SciTokens projects and co-PI of the Center for Trustworthy Scientific Cyberinfrastructure and the Software Assurance Marketplace. Jim also contributes to the LIGO, LSST, and XSEDE projects. Jim received his PhD in computer sciences from the University of Wisconsin-Madison.

Tony Baylis is the senior management advocate for diversity and inclusion for the Laboratory. Tony is responsible for overseeing the laboratory's interactions and successful execution in building, partnering and collaborating with governmental, educational, industrial, community interests and other stakeholders. LLNL has had a long history in working with Minority Serving Institutions, specifically relationships with American Indian Institutions, Hispanic Institutions, and Historically Black College and Universities. He represents the Laboratory on the subjects of Diversity and Inclusion, STEM, Outreach Efforts, and Student Programs.

Tony's career represents 31 years of administrative, project, program, technical, and organizational management. He has worked in a scientific and technical environment for over 23 years and has worked as a consultant in industry as well. Tony has extensive experience networking with a broad range of academic, industry, government and non-profit organizations that has educated him and helped him in his career. He is a DOE Minorities in Energy Champion for the department and also serves on a number of conference program committees and

advisory boards that promote STEM and diversity in science and technical careers.

Richard Biever is Duke University's chief information security officer and director of identity management. The IT Security Office facilitates IT security initiatives for the university, working closely with our counterparts in the Duke health system, and coordinates campus-wide security efforts through the Security Liaisons Group, which comprises IT security people from departments and schools across Duke. The identity management team manages Duke's electronic identities (also known as NetIDs) as well as the mechanisms used for user authentication and authorization.

Richard joined Duke in February 2011, after previously holding positions with the Georgia Institute of Technology's Office of Information Technology and Hewlett Packard.

Richard is an experienced security professional with SANS GIAC Certified Enterprise Defender (GSED) and Certified Information Systems Security Professional (CISSP) credentials. He holds a bachelor's degree in political science from the University of Georgia and a master's degree in international relations from Georgia State University.

Leslee A. Bohland serves as the Administrative & Finance Director at Indiana University's Center for Applied Cybersecurity Research (CACR). She is a graduate of the IU School of Business (B.S. '93).

Leslee comes to the CACR and CTSC from a background in Management, Finance and Accounting. She has worked with government divisions, as well as in the private sector.

Diana Borecky serves as the Events & Communications Manager at Indiana University's Center for Applied Cybersecurity Research (CACR). She has worked for IU for 19 years in the IU UITs Finance office, before joining CACR in 2016.

Robert (Bob) Cowles is a principal in BrightLite Information Security performing cybersecurity assessments and consulting in research and education about information security. He served as CISO at SLAC National Accelerator Laboratory (1997--2012); participated in the development of security policies and procedures for the LHC Computing Grid (2001--2008); and was an instructor at the University of Hong Kong in information security (2000--2003). A contributor to Indiana University's CACR since 2013, he participated in the XSIM project on identity management and has been working with CTSC since 2015. In 2017, he was honored to be named as a CACR Senior Fellow.

Sanchari Das is a PhD Student in the School of Informatics, Computing, and Engineering at Indiana University Bloomington. A security track researcher, her work includes studies in Usable Privacy and Security, User Experience, Social Media Research, and Human-Computer

Interaction. Her double Masters degrees were received from Indiana University Bloomington and Jadavpur University, Kolkata, India. She received her Bachelor's in Computer Applications from The Heritage Academy, Kolkata, India and was a Gold-medalist in her batch. She has also interned in prestigious organizations including Infosys Limited and HCL Technologies.

Erik Deumens is director for Research Computing in University of Florida Information Technology since 2011. He has a background in computational physics and has architected and written software for simulation of molecular reactions and structure. He is the architect of the super instruction architecture for scaling computational software to ten thousand CPU cores and hundred GPUs. Since 2015 he has been working on designing and implementing cyberinfrastructure for secure and compliant computing to meet FISMA and CUI requirements for research projects.

Emily Dillon is currently a technical engineering analyst for the Information Security department at Ascension Technologies. There her focus is on IoT/ medical device security and compliance. Emily is pursuing her Master of Science in Information Assurance and Cybersecurity.

Rion Dooley is principal investigator on the Agave Project a Science-as-a-Service API platform allowing researchers worldwide to manage data, run code, collaborate freely, and integrate their science anywhere. His previous projects span areas of identity management, distributed web security, full-stack application development, data management, cloud services, and high performance computing. Rion earned a Ph.D. in computer science from Louisiana State University. Rion actively puts his wife and two daughters at the top of his list of accomplishments. He hopes his work can someday edge out dancing teddy bears and smear-proof lipstick on their lists of favorite inventions.

Jeannette Dopheide is senior education outreach and training coordinator at NCSA. Her experience in education and outreach began as a high school teacher before moving onto business systems analysis and applications training for a commercial software company. Jeannette joined Trusted CI and NCSA in 2014 and works primarily on education outreach for projects that impact both Trusted CI and NCSA. Jeannette is a graduate of Illinois State University.

Leah Dorman is a student at the University of Maine-Augusta studying Business Management, with a concentration in Computer Information Systems. Many of her research and presentations have rooted from her work and interest in Cybersecurity. Along with being a student, she also works on the Information Systems Security team at Eastern Maine Healthcare

Systems, where her role has involved implementing an Identity & Access Management provisioning system, leading the user provisioning of several clinical, financial, and technical systems, as well as reviewing, testing, and implementing security plans and providing technical support, system documentation, and training materials to end users. Her career in Cybersecurity has led to the opportunity to present an Identity & Access Management Solution to other potential IAM customers as well as presenting at the Maine Science Festival, to make kids in the community both aware of the threats, but also to spark interest in possible future careers in the field. Identity & Access Management is so crucial to Cybersecurity now and due to her experience with it, it has become a passion of hers to help her company develop it further and use the automation functionality to its full advantage in order to cut down on internal risks.

Amy Friedlander was named Deputy Office Director in the Office of Advanced Cyberinfrastructure, Directorate for Computer and Information Science and Engineering (CISE/OAC) in January, 2016 where she had served as Acting Deputy Division Director since November, 2014. Since joining NSF in 2010, she has led several strategic activities, including SBE 2020, resulted in the widely-distributed report *Rebuilding the Mosaic* (2011), and coordination of NSF-wide activities for the Public Access Initiative.

Prior to her NSF appointment, Dr. Friedlander held positions in the non-profit and private sectors, which included establishing the Washington, DC cultural resource management office for an international consulting firm with a substantial nation-wide program in environmental management and compliance; leading the firm's first international preservation planning project; and serving as senior program manager for the DHS-funded DNSSEC deployment project. She participated in the Blue Ribbon Task Force on Sustainable Digital Preservation and Access, funded largely by NSF; led the initial strategic planning for the Library of Congress' National Digital Information Infrastructure and Preservation Program; and served as editor-in-chief of the *ACM Journal on Computing and Cultural Heritage*. At the Corporation for National Research Initiatives, she was the founding editor of *D-Lib Magazine* (www.dlib.org) and the author of a series of studies of the historical development large-scale technology infrastructures in the U.S.

Dr. Friedlander graduated from Vassar College, where she was elected to Phi Beta Kappa, and holds the M.A. and Ph.D. in History from Emory University and the M.S.L.I.S. from The Catholic University of America. She pursued postdoctoral work on quantitative methods and computer-assisted social science research at the Newberry Library in Chicago, IL.

Grayson Harbour is a member of the Class of 2019 at the Indiana University Maurer School of Law in Bloomington. He is also pursuing his masters degree in cybersecurity risk management.

His current work encompasses analyzing cybersecurity regulation and developing policy to ensure a secure, economic, and valuable IT environment for the scientific community at large. He is a graduate of the School of Journalism (B.A.J. 2015, Indiana University Bloomington) and a former Press Freedom Fellow at the International Press Institute in Vienna, Austria. Before law school Grayson was a writer and assistant to multiple documentary production companies in Los Angeles.

Elisa Heymann is a Senior Scientist at the Computer Sciences Department of the University of Wisconsin–Madison, and an Associate Professor in the Computer Architecture and Operating Systems Department at the Autonomous University of Barcelona (UAB). She co-directs the MIST software vulnerability assessment project in collaboration with her colleagues at the University of Wisconsin. Heymann is part of Trusted CI, the NFS cyber security center for excellence, where she works on Software Assurance training and engagements.

Heymann carries out training in universities, companies, and conferences around the world. Heymann's research interests include security and resource management for Grid and Cloud environments, and cyber–security in transportation. Her research is supported by NSF, the Spanish government, the European Commission, and NATO. Heymann received her M.S. and Ph.D. degrees in Computer Science from the Autonomous University of Barcelona (Spain) in 1995 and 2001 respectively.

Florence Hudson is on the Program Committee for the 2018 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure. She is Special Advisor for Next Generation Internet at the Northeast Big Data Innovation Hub at Columbia University, on the Editorial Board for the journal Blockchain in Healthcare Today, Co-Founder of the IEEE-ISTO Blockchain in Healthcare Global, and Founder & CEO of Florence D. Hudson International, LLC, consulting on advanced technology and diversity & inclusion. Hudson was PI for the NSF SaTC EAGER: Cybersecurity Transition to Practice (TTP) Acceleration (NSF award 1650445). Through this EAGER, Florence worked with a team to bring together cybersecurity researches with CI and cybersecurity practitioners including CIOs, CISOs, industry, regional networks and start-ups to enable collaboration and matchmaking between cybersecurity researchers and practitioners, creating opportunities to accelerate cybersecurity research transition to practice. Formerly an IBM Vice President and Chief Technology Officer, and Internet2 Senior Vice President and Chief Innovation Officer, she earned a BSE in Mechanical and Aerospace Engineering at Princeton University, and attended executive education at Harvard Business School and Columbia University.

Craig Jackson (scjackso@iu.edu) is Chief Policy Analyst at the Indiana University Center for

Applied Cybersecurity Research (CACR), where his research interests include information security program development and governance, cybersecurity assessments, legal and regulatory regimes' impact on information security and cyber resilience, evidence-based security, and innovative defenses. He is a Co-PI of the NSF Cybersecurity Center of Excellence, and leads CACR's collaborative efforts with Naval Surface Warfare Center Crane, where he is presently employed as temporary faculty. He is a co-author of *Security from First Principles: A Practical Guide to the Information Security Practice Principles*. Craig is a graduate of the IU Maurer School of Law, IU School of Education, and Washington University in St. Louis. In addition to his litigation experience, Craig's research, design, project management, and psychology background includes work at the IU Center for Research on Learning and Technology and the Washington University in St. Louis School of Medicine.

Ryan Kiser is a System Analyst at the Indiana University Center for Applied Cybersecurity (CACR) and Trusted CI. Ryan comes to CACR and Trusted CI from a system administration and small business consulting background. In addition to his role with Trusted CI, his current responsibilities include performing security assessments for public and private sector IT systems as well as risk assessment and regulated data efforts for Indiana University's central IT systems.

Charley Kneifel, PhD, is Senior Technical Director at OIT. He joined Duke University in 2012. Dr. Kneifel manages Duke's central technology infrastructure and Software Defined Networking Project. He has coordinated several technology grants at Duke including the National Science Foundation's Data Infrastructure Building Blocks (DIBBS) grant to build campus cyber infrastructures.

Prior to working at Duke, Dr. Kneifel was chief information officer at the American Kennel Club for nine years. He has also held multiple technical positions at NC State University. Dr. Kneifel holds a B.S. in Chemistry from Carnegie Mellon University and a Ph.D. in Chemistry from the State University of New York at Stony Brook.

Richard Knepper is Deputy Director of the Cornell University Center for Advanced Computing, which provides the Red Cloud private cloud service for Cornell, and is the leading institution of the Aristotle Federated Cloud program, one of the NSF's Data-Intensive Building Blocks Programs. In his role at the CAC, Dr. Knepper works to help Cornell researchers meet their computational needs and is manager of the NSF XSEDE project's Cyberinfrastructure Resource Integration team. In his research, Dr. Knepper examines the virtual organizations supporting large-scale cyberinfrastructure, their evolution and support of science disciplines over time.

Mark Krenz is the Lead Security Analyst at Indiana University's Center for Applied Cybersecurity Research with over two decades of experience in information security and system

administration spread across multiple sectors. His interests at CACR include policy development, operational security development, security auditing and security education. He studied Computer Science and Mathematics at Indiana University.

John Michael Lowe is the senior engineer for the National Science Foundation's Jetstream project. He has been working in HPC, virtualization, and cloud computing at Indiana University for the past 12 years.

James A. Marsteller, Jr. is the Pittsburgh Supercomputer Center Chief Information Security Officer. He has extensive security leadership experience with the TeraGrid and XSEDE security operations team and is a Co-PI for the Center For Trustworthy Scientific Cyberinfrastructure, the NSF Cybersecurity Center of Excellence. James also has served as the program chair for annual NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure since 2007. He has also served on the board of directors for the Pittsburgh chapter of the FBI Infragard program for many years. He holds a Master of Information Technology Management from Carnegie Mellon University and is a Certified Information Systems Security Professional.

Dr. Ashwin J. Mathew is a visiting scholar and lecturer at the UC Berkeley School of Information, a fellow at the Slow Science Institute, and a researcher at Packet Clearing House. He studies trust and coordination problems in the operation of Internet infrastructure, focusing on the relationships, practices, and institutions of the Internet's technical personnel. He holds Ph.D. and Masters degrees from the UC Berkeley School of Information. Prior to his doctoral work, Dr. Mathew spent a decade working as a software engineer and technical architect in companies such as Adobe Systems and Sun Microsystems.

Kim Milford began serving as Executive Director of REN-ISAC in April 2014. She works with members, partners, sponsors, and advisory committees to direct strategic objectives in support of members, providing services and information that allow higher educational institutions to better defend local technical environments and is responsible for overseeing administration and operations.

Since joining Indiana University in June 2007, Ms. Milford has served in several roles leading strategic IT initiatives. As Chief Privacy Officer, she coordinated privacy-related efforts while serving on IU's Assurance Council, chairing the Committee of Data Stewards, and directing the work of the University Information Policy Office including IU's IT incident response team. From 2005 – 2007, Ms. Milford worked as Information Security Officer at the University of Rochester leading an information security program that included disaster recovery planning, identity

management, incident response, and user awareness. In her position as Information Security Manager at University of Wisconsin-Madison from 1998 - 2005, she assisted in establishing the university's information security department and co-lead in the development of an annual security conference.

Ms. Milford provides cybersecurity, information policy, and privacy expertise and presentations at national and regional conferences, seminars and consortia. Ms. Milford has a B.S. in Accounting from Saint Louis University in St. Louis, Missouri and a J.D. from John Marshall Law School in Chicago, Illinois.

Barton Miller the Vilas Distinguished Achievement Professor and the Amar and Belinder Sohi Professor in Computer Sciences at the University of Wisconsin-Madison. He is Chief Scientist for the DHS Software Assurance Marketplace research facility. He codirects the MIST software vulnerability assessment project in collaboration with his colleagues at the Autonomous University of Barcelona. He also leads Paradyn Parallel Performance Tool project, which is investigating performance and instrumentation technologies for parallel and distributed applications and systems. His research interests include systems security, binary and malicious code analysis and instrumentation extreme scale systems, and parallel and distributed program measurement and debugging.

Miller's research is supported by the U.S. Department of Homeland Security, U.S. Department of Energy, National Science Foundation, NATO, and various corporations. In 1988, Miller founded the field of Fuzz random software testing, which is the foundation of many security and software engineering disciplines. In 1992, Miller (working with his then student, Prof. Jeffrey Hollingsworth) founded the field of dynamic binary code instrumentation and coined the term "dynamic instrumentation". Dynamic instrumentation forms the basis for his current efforts in malware analysis and instrumentation.

Miller was the chair of the IDA Center for Computing Sciences Program Review Committee, a member of the Los Alamos National Laboratory Computing, Communications and Networking Division Review Committee, and has been on the U.S. Secret Service Electronic Crimes Task Force (Chicago Area), the Advisory Committee for Tuskegee University's High Performance Computing Program, and the Advisory Board for the International Summer Institute on Parallel Computer Architectures, Languages, and Algorithms in Prague. Miller received his Ph.D. degree in Computer Science from the University of California, Berkeley in 1984. He is a Fellow of the ACM.

Austin Mitts is the Information Technology Support Specialist for Indiana University's Center for Applied Cybersecurity Research (CACR). He has been with CACR and Trusted CI since March

2018. Austin has a Bachelor's Degree in Informatics from Indiana University's School of Informatics and Computing.

Laura Paglione is an entrepreneurial, technically versatile, resourceful leader who thrives at the intersection of creative, technical and business environments. She currently serves as the Director of Strategic Initiatives, and was formerly the Technical Director of ORCID, where she directed the technical efforts in ORCID's mission to address name ambiguity for researchers, and serve as a gateway to connect their research activities from disparate sources. Previously as Director, Advancing Innovation at the Kauffman Foundation, Laura directed the efforts of the iBridge Network, an innovation catalyst for university collaboration and technology commercialization. In prior positions at Ford Motor Company and Avid Technology, as well as several start-up/gazelle companies, Laura has turned around, launched and led 4 other high-profile initiatives, the most visible of which was for Ford Motor Company's Board of Directors.

Susan Ramsey is a Risk Assessor and Security Engineer at the National Center for Atmospheric Research. She has over twenty years of experience building enterprise infrastructure and cloud computing. She joined NCAR in 2014 and promptly launched multiple initiatives to tackle compliance and identity management. Her latest projects include building a FISMA moderate segment and an organization wide Continuous Monitoring Plan. She has an MS in Computer Information Technology from Regis University, (thesis on Vulnerability Assessment). She is currently working towards a second Master of Science degree, in Information Security Engineering, from SANS Technical Institute.

Preston Ruff is a senior undergraduate student who studies computer science at New Mexico Tech. He has been seen researching orthopedic instrument patents and acting as a consultant to evaluate the usability of a concept mapping application. Also, he previously managed the New Mexico Tech Inventors and Entrepreneurs conference website for a time. Preston enjoys riding his bike and writing elaborate plans for DIY microcontroller systems such as thermostats or garden watering systems that he never seems to have enough time to implement. Recently he has been conducting research for TrustedCI with the goal of creating a due care cybersecurity reference for software developers to better mitigate software weaknesses during the development phase.

Scott Russell (scolruss@indiana.edu) is a Senior Policy Analyst with the Indiana University Center for Applied Cybersecurity Research (CACR), where his work focuses on the improvement of federal privacy and cybersecurity policy. A lawyer and researcher, Scott specializes in privacy, cybersecurity, and international law, and his past research has included principled

cybersecurity, cybersecurity assessments, cybersecurity due diligence, cybersecurity self-governance, international data jurisdiction, and constitutional issues on digital surveillance. He is a co-author of *Security from First Principles: A Practical Guide to the Information Security Practice Principles*, and a key contributor to CACR's collaborative efforts with Naval Surface Warfare Center Crane. He received his B.A. in Computer Science and History from the University of Virginia, received his J.D. from Indiana University, interned at MITRE, and served as a postdoctoral fellow at CACR.

Phil Salkie is a computer scientist who has been working as an industrial controls and automation engineer since 1984. His software and hardware designs serve sectors as diverse as food packaging, broadcast television, emergency power generation, water purification, sewage processing, medical device manufacturing, and UV photochemistry. He is managing partner of Jeneriah Industrial Automation, designing, supporting, and securing PLC, HMI, and SCADA systems, as well as embedded controllers using Linux and RTOS. He was honored to present the lunch Keynote address at the 2017 CACR CyberSecurity Summit - "Automation: Ready or not, here it comes."

Anurag Shankar is a senior security analyst at Indiana University's Center for Applied Cybersecurity Research (CACR). His expertise includes regulatory compliance (HIPAA, FISMA, CUI) and cybersecurity risk management. He has helped numerous institutions tackle HIPAA compliance and is responsible for developing a NIST based risk management framework and using it to align IU's central research and enterprise cyberinfrastructures with HIPAA. His prior engagements include nearly twenty years with IU's central IT organization developing, delivering, and managing Unix support, massive data storage, the national Teragrid project, and supporting the research mission of the IU School of Medicine. He played a key role in building IU's research data storage environments, for supporting IU's Indiana Genomics Initiative and other life sciences efforts, and for creating information infrastructures and technology solutions for the Indiana Clinical and Translational Sciences Institute (CTSI). He is a computational astrophysicist by training (Ph.D. University of Illinois, '90).

Adam Slagell received an M.S. in computer science from the University of Illinois at Urbana-Champaign in 2003, a masters degree in mathematics from Northern Illinois University (NIU) in 2000, and a B.S. in mathematics from NIU in 1999. He currently serves as the director of the Cybersecurity and Networking Division and Chief Information Security Officer at the National Center for Supercomputing Applications (NCSA) where he co-leads the security office for the NSF-funded XSEDE project, serves on the University of Illinois IT Leadership Team Security Working Group, and is a co-PI for the NSF Bro Center of Excellence, which brings its network security monitoring expertise and support to NSF-funded cyber-infrastructure and

Higher Ed.

Susan Sons serves as Chief Security Analyst at Indiana University's Center for Applied Cybersecurity Research, as well as ISO (Information Security Officer) for NSF-funded Open Science Grid and senior personnel on the Software Assurance Marketplace and Trusted CI, the NSF Cybersecurity Center of Excellence. Susan co-authored the Information Security Practice Principles, a touchstone for teaching security professionals and non-security personnel to deal with cybersecurity on a first-principles basis, along with CACR colleagues Craig Jackson and Scott Russell. She is also currently President of the Internet Civil Engineering Institute, a nonprofit dedicated to supporting the development and stewardship of reliable, secure, and open source internet infrastructure software. More on Susan's projects can be found at <https://security.engineering>.

Victoria Stodden is an associate professor in the School of Information Sciences at the University of Illinois at Urbana-Champaign, with affiliate appointments in the School of Law, the Department of Computer Science, the Department of Statistics, the Coordinated Science Laboratory, and the National Center for Supercomputing Applications. She is also a faculty affiliate of the Center for Informatics Research in Science and Scholarship (CIRSS) in the School of Information Sciences at the University of Illinois.

Victoria completed both her PhD in statistics and her law degree at Stanford University, and graduated magna cum laude from the University of Ottawa.

Jeremy Straub is the Associate Director of the NDSU Institute for Cyber Security Education and Research and an Assistant Professor in the Department of Computer Science at the North Dakota State University. He is also an Editor-in-Chief for the Journal of Cybersecurity and Privacy. Straub holds a Ph.D. in Scientific Computing, an M.S. and an M.B.A. and two B.S. degrees. Straub's research spans the gauntlet between technology development, technology policy and commercialization. It has recently focused on cyber-physical system security, robotic command and control, aerospace command and 3D printing quality assurance.

Steven Tuecke is co-founder and director of Globus (www.globus.org), with a focus on delivering commercial-quality, cloud-based software application and platform services to global, non-profit research communities, as a sustainable, non-profit business within the University of Chicago (UC). From 2009-2016, Tuecke was also Deputy Director of the Computation Institute at UC. Prior to UC, Steven was co-founder, CEO and CTO of Univa

Corporation from 2004-2008, providing open source and proprietary software for the high-performance computing and cloud computing markets. Before that, he spent 14 years at Argonne National Laboratory as research staff. Tuecke graduated with a B.A in mathematics and computer science from St. Olaf College.

Romain Wartel has been fighting botnets and bad actors for many years, while protecting the Worldwide LHC Computing Grid. This distributed cyber-infrastructure, supporting CERN's Large Hadron Collider, spans across hundreds of organizations worldwide. Romain specializes in large-scale security intrusions, affecting multiple organizations and mission critical services. This implies focusing on malware, malicious infrastructures, forensics, threat intelligence, and building international collaborations to prepare for and manage crises. Beside operational security, Romain is involved in identity federation, and he also leads a CERN project focusing on modern hardware adoption, called Techlab.

Von Welch is the director of the Indiana University Center for Applied Cybersecurity Research. CACR has a unique focus - improve real world cybersecurity for organizations with missions that challenge for traditional cybersecurity approaches. Examples include research and development, open science, and highly distributed collaborations. CACR project partners and funders include the US Department of Defense, National Science Foundation, Department of Homeland Security, as well as private sector organizations - and Von's roles span research, development, operations, and leadership.

Brett Zupan is a Security Analyst & D.C. Liaison for the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC) and a Risk Analyst at Gate 15, with experience in all-hazards analysis, exercise development, and information sharing. He has supported analysis, preparedness, and operations for a number of critical infrastructure communities, including Higher Education, the Water and Wastewater Systems Sector, and the Commercial Facilities Sector, among other projects. Before joining Gate 15 in 2016, he worked at the Georgia State Senate. Brett received his Masters of International Relations from American University.

Appendix E: Student Feedback

Final Thoughts on Attending the Summit

As described in Section 7.2, the students who attended the Summit were part of a scholarship program organized and funded by Trusted CI. They were asked to share feedback on their experiences with the Summit and Student Program. Their responses are printed below.

Sanchari Das:

My name is Sanchari and I am a doctoral student in the School of Informatics, Computing, and Engineering at Indiana University Bloomington, specializing in Usable Privacy and Security. I think this summit was a great opportunity to meet researchers and practitioners from other organizations. I thoroughly enjoyed their perspective, and insights in the discipline of cybersecurity and gathered knowledge to pave my future research directions. Given the diverse research areas which was covered, this truly was a golden opportunity to broaden a graduate student's vision, such as myself, understanding more about usable privacy and security.

The NSF cybersecurity summit provided the perfect blend of academicians and those working in industry, who do and preach cybersecurity practices and direct their research accordingly. Given the workshops and talks that was conducted in the summit, it was not limited to discuss cybersecurity infrastructure, but also discussed about the users who are a major part, are affected, and contribute to follow cybersecurity practices. It was one of the gathering where practitioners from the industry likewise joined to discuss around the applications of such research.

As a student I learned about the current challenges in the field of cybersecurity, how usable security and privacy is slowly but surely making its marking where we all aim in not keeping the humans out of the loop but making them aware through simple but informative tools. I also learned how people from different field such as, law (policy makers), software developers, security engineers, academicians can all work together to help build a secure environment to protect data of an organization or individual.

Apart from interesting ideas, I would particularly like to thank my mentor Mark Krenz and Jeannette Dopheide, who made the process smooth and helped me throughout my stay and helped me interact with eminent researchers and practitioners in my field. I enjoyed the workshops I was involved in as well, Susan Son's insights on the different version controls and monitoring old patches to find loopholes which can be played further was interesting.

I would also like to thank Von Welch, the director of Indiana University's Center for Applied Cybersecurity Research who is extremely approachable and helps every student to

achieve their best in this field through such initiatives.

Grant Allard:

The Trusted CI/NSF 2018 Cybersecurity Summit provides an outstanding opportunity to professionally and scholastically improve my understanding of the key issues in scientific cyberinfrastructure. The Trusted CI leadership team makes you, as a student, feel welcome and helps you to explore the pressing challenges facing the scientific cyberinfrastructure community today. The mentoring initiative associated with the student program is a superb educational tool that helped me put my experience in context and learn from one of the leaders of this field. One of my big takeaways from the week together is the importance that we as students will play to the scientific cyberinfrastructure community as we enter the scientific workforce: cybersecurity is not only a concern for CISOs but for the entire scientific community. The academic community owes a huge debt of gratitude to our CISOs for helping us keep our data secure, accessible, and integral.

I am taking what I learned from this conference and using it to develop a white paper and I identify how I, as an aspiring scholar of public policy, can contribute to the community. This conference also has given me multiple opportunities at my university to meet new people and contribute to new efforts. This experience was exactly how a student program should be--in my opinion--and I highly recommend it to students of all levels or to advisors who are looking to promote their students' growth."

Preston Ruff:

I enjoyed the close-knit, friendly, and informative experience of the NSF summit. There I was able to test my text parsing skills in a log analysis workshop and I was exposed to the mystery of industrial control systems. Thank you to everyone at Trusted CI for hosting the event. I'm grateful to have met such brilliant people who work to create the cybersecurity systems and policy of tomorrow.

Maggie Ahern:

Attending the NSF 2018 Cybersecurity Summit was a fantastic learning experience. I have always been interested in cybersecurity, but this summit gave insight into the field that I had never been exposed to before. Some of the highlights include Software Engineering Best Practices and Legal Policy on Cybersecurity. I also particularly enjoyed the breakout session we had during lunch where we could discuss different topics of interest. I sat at a table that discussed books with the theme of cybersecurity and I went home with a few recommendations. The Student Program also connected us with a mentor for the duration of the conference. My mentor was incredibly understanding, knowledgeable, and inspiring. She is

someone that I really admire and strive to live up to one day. Without this opportunity I probably would not have gotten to meet her, or all the other amazing individuals that I was able to interact with during the summit. All in all, I am incredibly grateful that I was given this opportunity to learn more about this subject and meet new individuals passionate about cybersecurity.

Leah Dorman:

At the NSF Cybersecurity conference, I immediately noticed a coherent understanding of cybersecurity's crucial role in science as well as a collaborative effort to produce trustworthy technology. The Trusted CI program committee did an excellent job putting on this event and as a student I felt very welcomed and was provided with the information and resources needed to enhance my cybersecurity knowledge and research skills. The first day was a training day. I attended Automated Assessment Tools – Theory & Practice which was about injection attacks (one of the most common vulnerabilities) and had hands-on training using source code analysis tools to find code errors and flaws. Then I attended Security Log Analysis Training which included ideas to improve security logging & monitoring as well as command examples that you can customize on your own logs and how to analyze data and look for patterns. This hands-on training provided me with valuable experience that would only improve my cybersecurity skills.

The next two days there were several presenters that covered topics such as

- Security Best Practices for Academic Cloud Service Providers (a big one I took away from this was Identity Access Management-aware Continuous Integration/Continuous Delivery Services)
- Involving Students in Cybersecurity for CI
- Silent Librarian (series of phishing attacks)
- Responding to advanced threats as a global community (building a trust relationship in cybersecurity community)
- XSEDE lessons learned (importance of multi-factor authentication)
- Incident Response Communications
- Password Adventures for a VO
- A case study on implementing crowdsourced threat intel and active response

Overall, the focus was on being Proactive vs being Reactive; changing the focus of cybersecurity from protecting (specifically against malicious attacks) to enabling - moving beyond the fear of data breach and focusing on how to better enable end users to deal with data theft and how to be ready to respond to events like that.

I am very thankful for the knowledge I gained at this conference. Thank you, Trusted CI, for

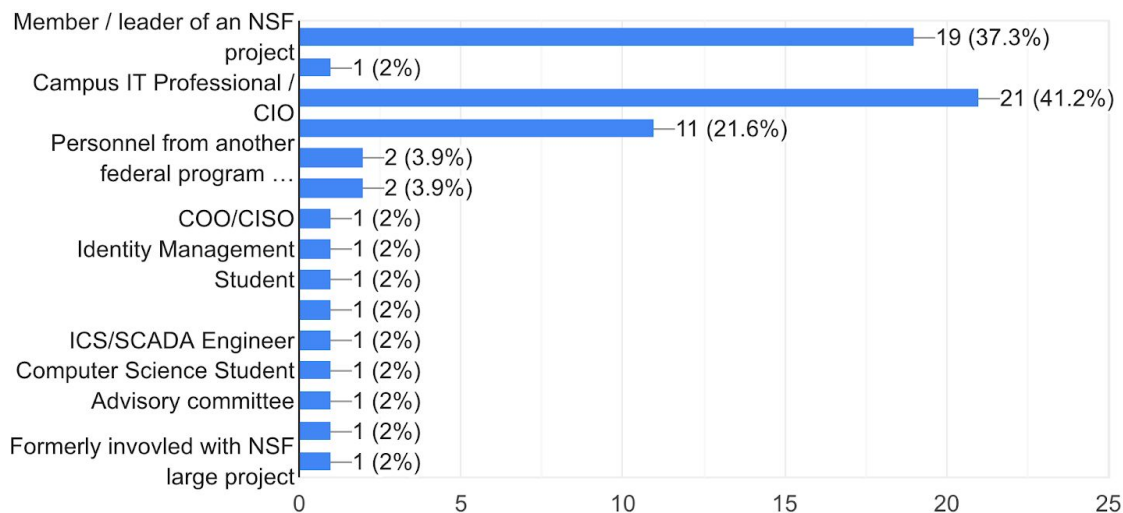
allowing me to participate as a student and for the engaging conversations and presentations that challenged and enhanced the way I think about cybersecurity.

Appendix F: Attendee Survey Summary Report

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

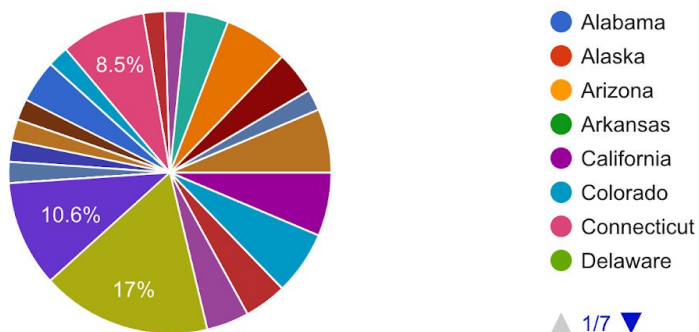
Which options best describe your job or position? Check all that apply.

51 responses



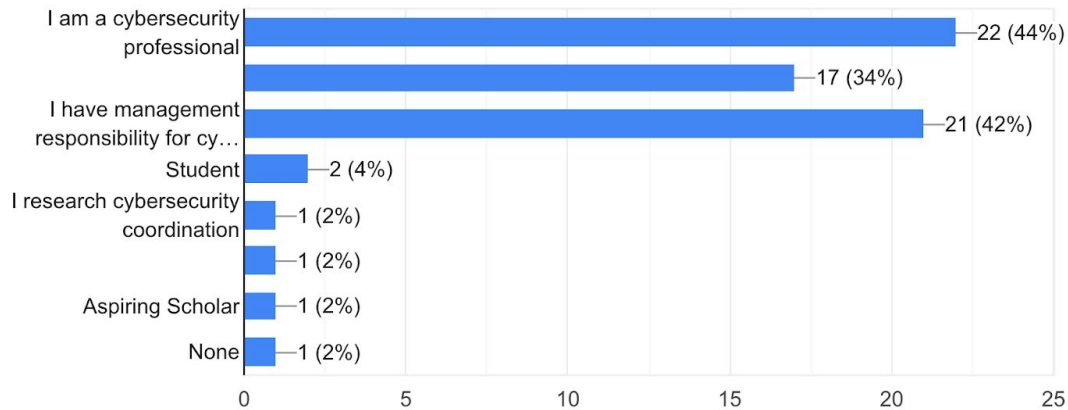
Where do you work primarily?

47 responses



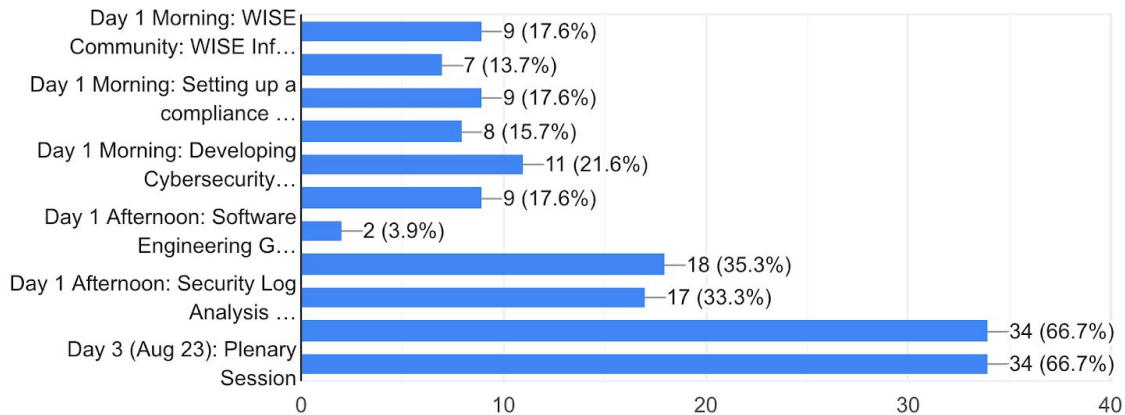
How would you characterize your job in relationship to cybersecurity? Please check all that apply.

50 responses



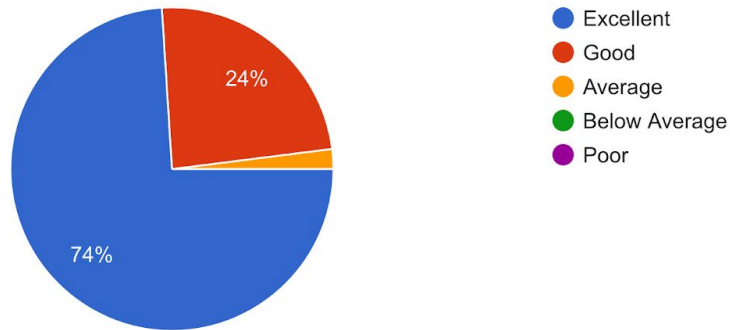
What sessions of the summit did you attend? Check all that apply.

51 responses

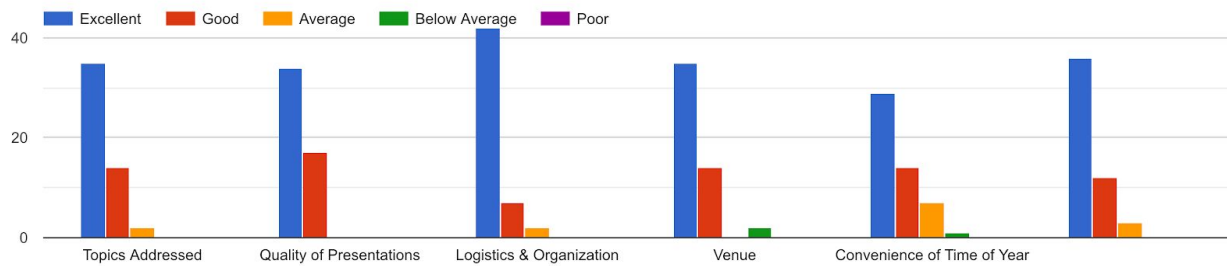


How would you rate your overall experience with the 2018 summit?

50 responses

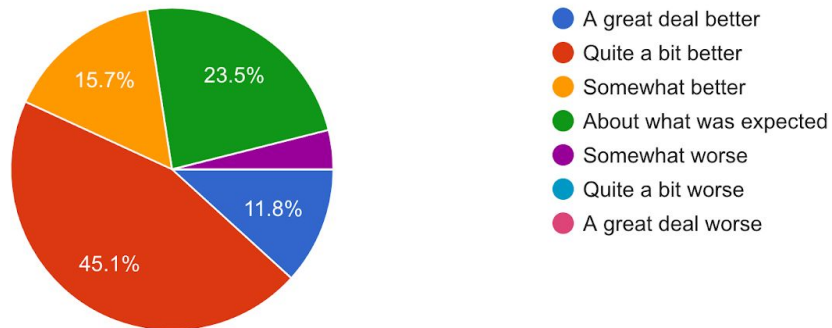


Please rate your experience with the 2018 summit in these areas:



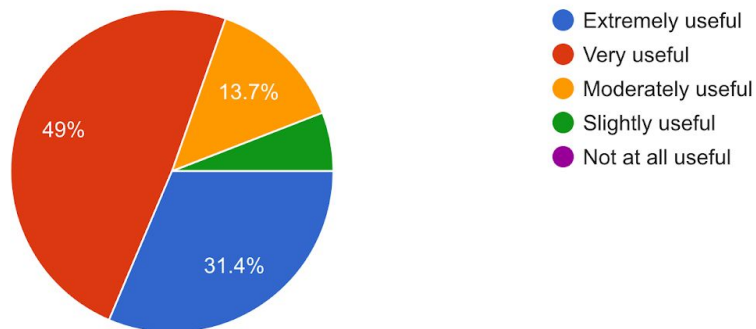
Was this summit better than what you expected, worse than what you expected, or about what you expected?

51 responses



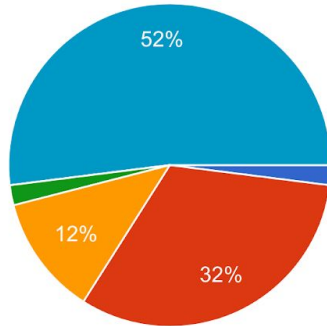
How useful to your work was the information discussed at the summit?

51 responses



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

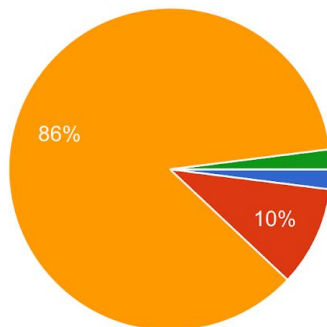
50 responses



- This year's summit was much better than last year's.
- This year's summit was better than last year's.
- This year's summit was about the same as last year's.
- This year's summit was worse than last year's.
- This year's summit was much worse than last year's.
- I did not attend last year's summit.

How would you describe the balance between structured presentations and informal networking opportunities?

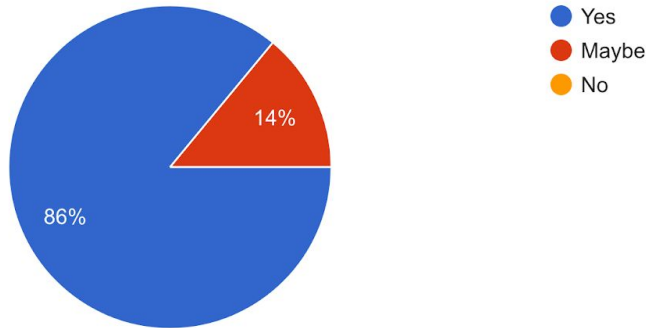
50 responses



- Much too little time for informal networking
- Too little time for informal networking
- About the right balance
- Too little time for structured presentations
- Much too little time for structured presentations

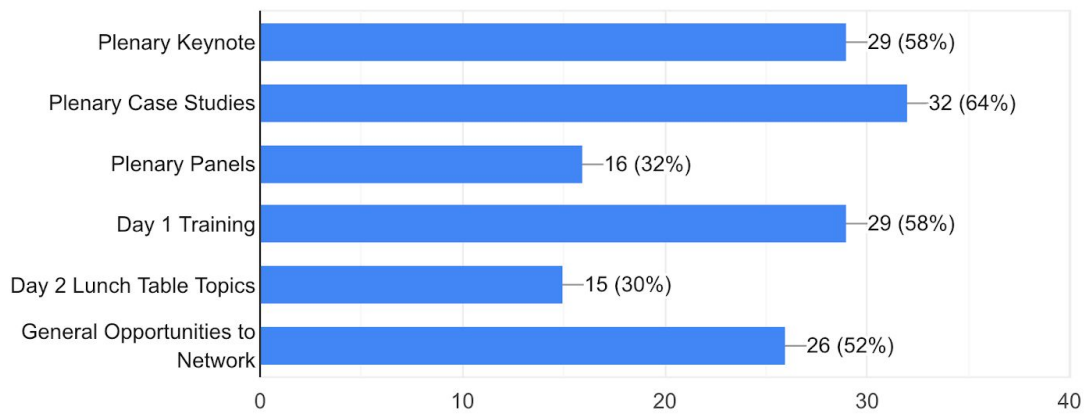
Would you like to attend future summits?

50 responses



What presentation format(s) did you find most valuable? (You may select more than one.)

50 responses

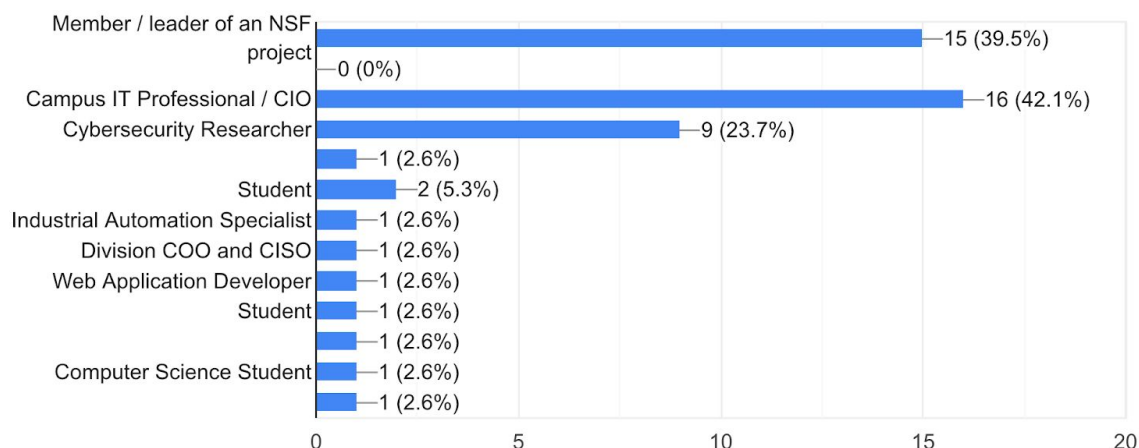


Appendix G: Training Evaluation Summary Report

Below are the collected responses from the Training Evaluation survey, displayed at charts.

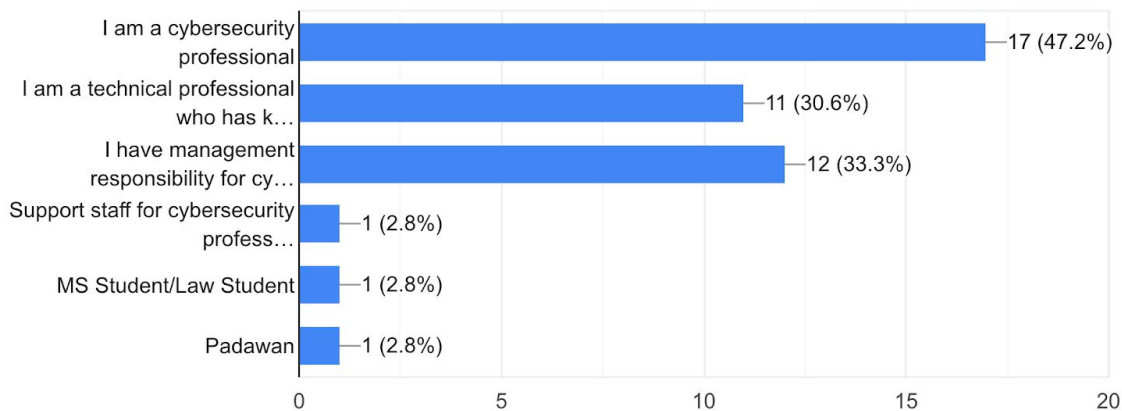
Which options best describe your job or position? Check all that apply.

38 responses



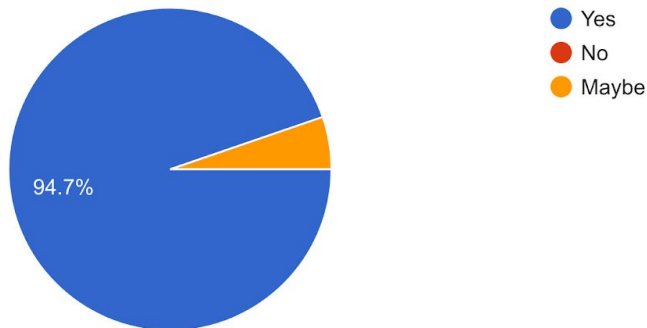
How would you characterize your job in relationship to cybersecurity? Please check all that apply.

36 responses



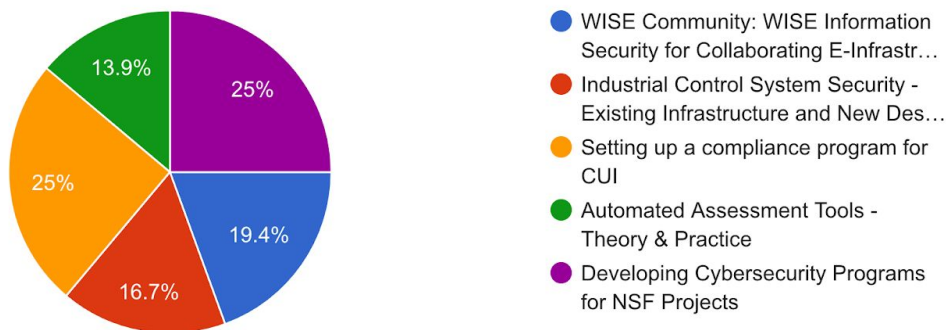
Based on your overall experience with the August 21st training sessions, would you participate in training offered at future summits?

38 responses



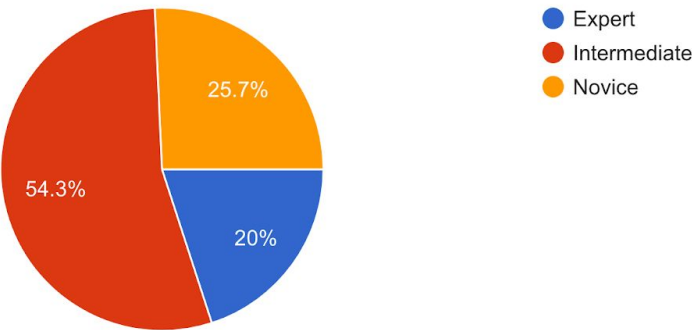
Which morning session did you attend?

36 responses



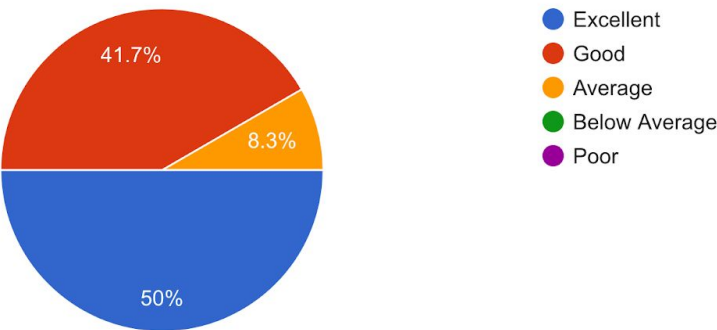
How would you rate your level of pre-training familiarity with the topics covered by this morning training session?

35 responses

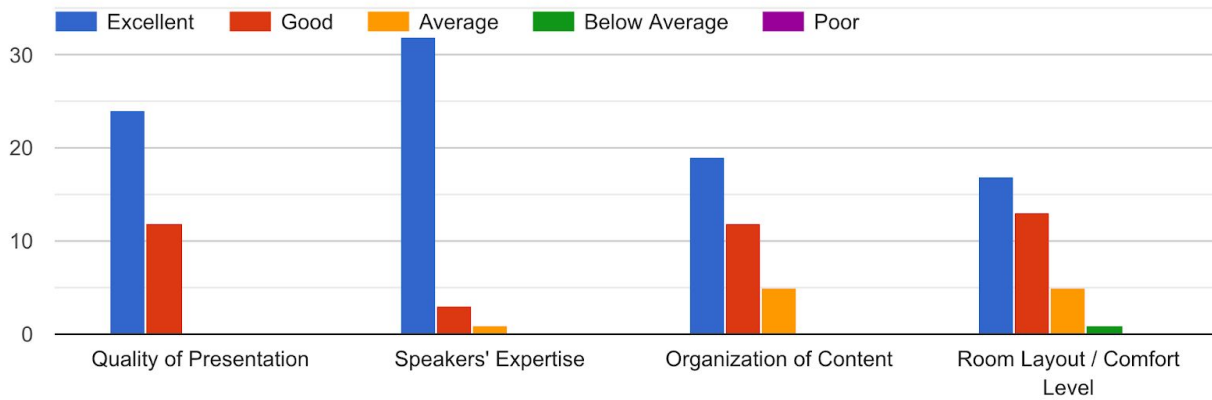


How would you rate your overall experience with the morning training?

36 responses

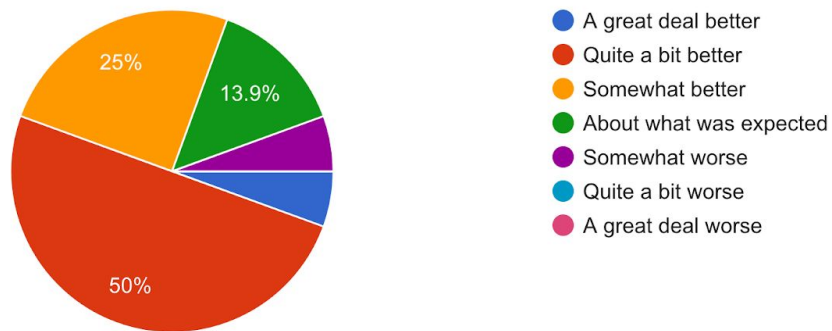


Please rate your experience with the morning training in these areas:



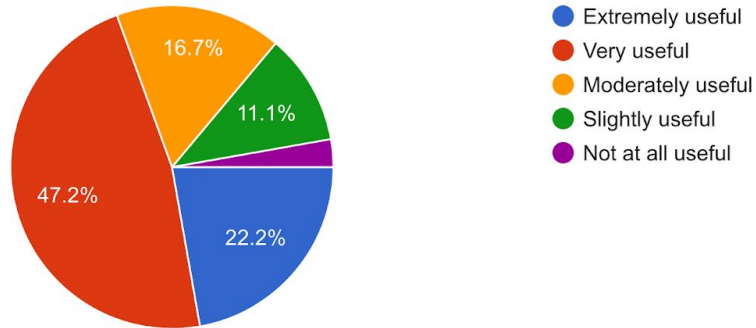
Was this morning training better than what you expected, worse than what you expected, or about what you expected?

36 responses



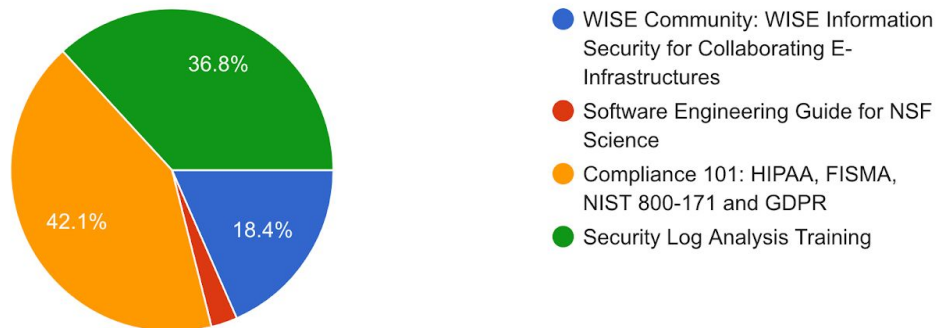
How useful to your work was this morning training?

36 responses



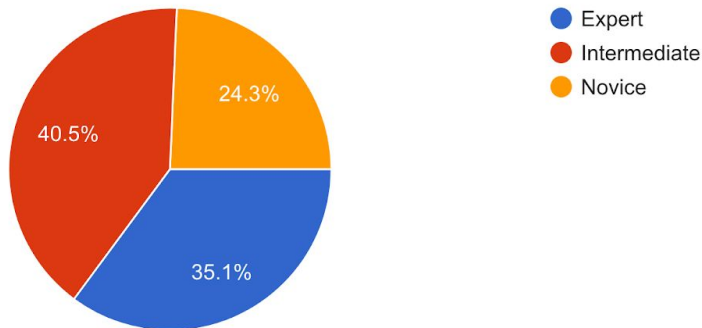
Which afternoon session did you attend?

38 responses



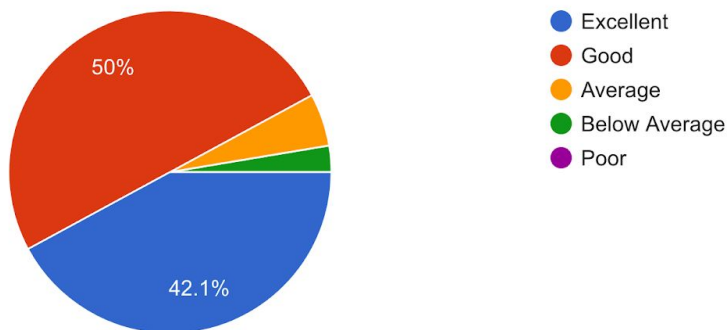
How would you rate your level of pre-training familiarity with the topics covered by this afternoon training session?

37 responses

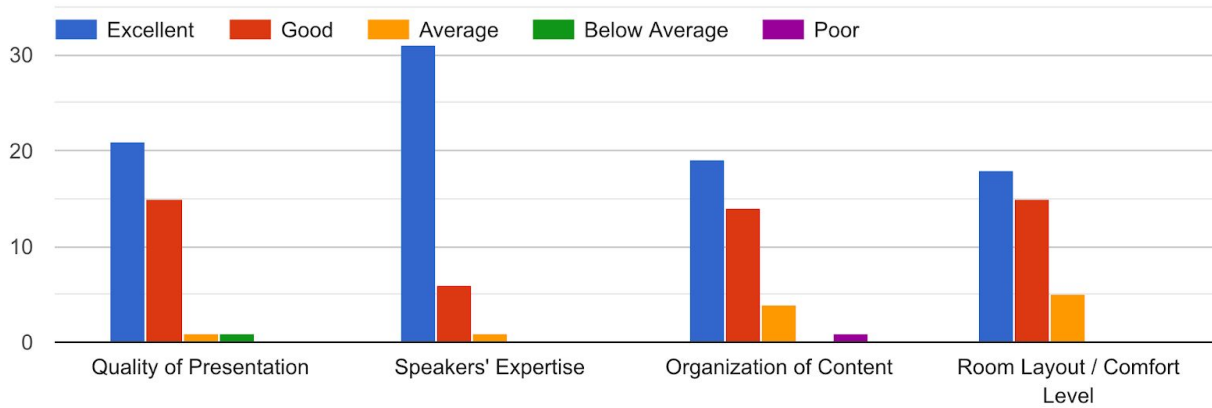


How would you rate your overall experience with the afternoon training?

38 responses

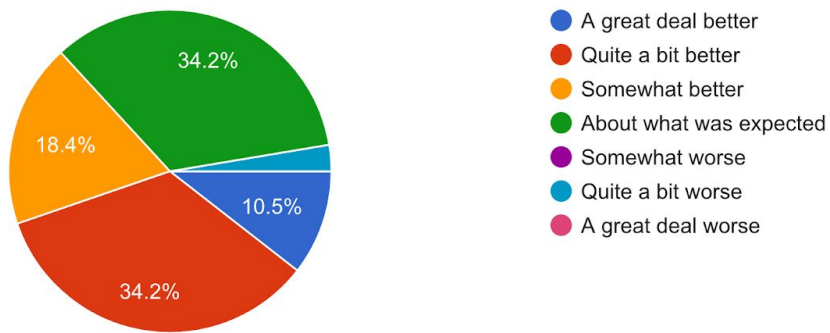


Please rate your experience with the afternoon training in these areas:



Was this afternoon training better than what you expected, worse than what you expected, or about what you expected?

38 responses



How useful to your work was this afternoon training?

38 responses

