Report of the 2015 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure

Understanding the Information Assets that Enable Science

August 17 - August 19

Westin Arlington Gateway - Arlington, VA

http://trustedci.org/2015summit

January 12, 2016

For Public Distribution

Craig Jackson, James Marsteller, Amy Starzynski Coddens, Von Welch

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 2015 Program Committee (highlighted in Section 3), 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 1234408. 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

Drafts of this report were circulated for comment to the Program Committee (December 3, 2015) and summit participants (December 10, 2015).

Citing this Report

Please cite as: Craig Jackson, Amy Starzynski Coddens. Report of the 2015 NSF Cybersecurity Summit for Cyberinfrastructure and Large Facilities: *Large Facility Cybersecurity Challenges and Responses*. http://hdl.handle.net/2022/20539

For the latest information on the Summit

Please see, http://trustedci.org/summit/

Table of Contents

Executive Summary

The 2015 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure served to build a trusting, collaborative community working to address core cybersecurity challenges in support NSF science. The 2015 summit built on the success, findings, and lessons learned from the 2014 event, and focused on the theme of *Understanding the Information Assets that Enable Science*. The Program Committee and community members drove the program, and despite this being only the second year for the Call For Participation (CFP), we saw a significant growth in number of submissions compared to the prior year. . The CFP resulted in seventeen (17) proposals including 1 case study presentation, 3 panel topics, 6 training sessions, 3 keynotes from the cybersecurity community at large, and 4 presentations from key leaders from within the NSF community. With such a strong response from the community to the CFP, we had more proposals than available time in the program.

The 2015 summit took place in Arlington, VA, August 17th through midday August 19th. On August 17th, it offered a full day of training. The second and third days followed were plenary sessions designed to address the theme of Understanding the Information Assets that Enable Science in the context of cyberinfrastructure projects and Large Facilities.

Ninety (90) individuals attended the summit, with 51 individuals -- over one half of all registrants -- participating in planning, speaking, providing training, co-authoring a CFP submission, and/or leading a lunch "table talk." In all, 50 NSF-funded projects, including 14 Large Facilities, were represented. Attendee evaluations and feedback were overwhelmingly positive and constructive.

Section 7 of this report includes twelve recommendations to the NSF CI and Large Facilities community. Each recommendation is derived from the summit's presentations and discussions, and is followed by a discussion of supporting evidence. These include Priority Recommendations (7.1), Recommendations for Continued Action (7.2), and Opportunities and Recommendations for Exploration (7.3). These recommendations will drive planning for the 2016 summit and the Center for Trustworthy Scientific Cyberinfrastructure's ongoing leadership efforts. More detail is in Section 7.

The following Priority Recommendations (*see*, 7.1) require focused attention to ensure that projects and facilities have sufficient resources, information security governance structure, and positions on software assurance requirements to make effective information security programs a reasonable possibility.

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.

1 Background: Evolving Cybersecurity Landscape, and Advancing Trustworthy Science

Cybersecurity is a fast-developing and challenging field for all organizations in our contemporary world. The challenge is amplified by the intersection of myriad factors, including rapidly changing technology; ever-evolving and diverse threats; lagging workforce development; economic challenges; asymmetries in the cost and difficulty of attack and defense; and the nascent state of cybersecurity practice in general.

NSF awardees face distinct questions when initiating information security programs due to their projects' unusual, and often unique, combination of attributes: distributed, collaborative organizational structures and relationships with other entities (*e.g.*, campus); unique, costly scientific instruments; limited resources, talent availability, and timelines; diversity in communities and missions; open, yet irreplaceable scientific data with an unclear threat model; and the need for reproducibility and maintaining public trust in their resulting science.

A number of well-known frameworks for cybersecurity exist, but they continue to evolve and none have emerged as a clear best practice. For example, NIST's *Framework for Improving Critical Infrastructure Cybersecurity*[1] and the National Strategy for Trusted Identities in Cyberspace (NSTIC)[2] propose important approaches for cybersecurity programs and identity management. However, best practices for the federal government, commercial companies, and even research labs and institutions of higher education, do not directly translate to scientific communities and computing infrastructure.

In addition to the cybersecurity efforts and experiences of individual NSF projects, and the research advances of the NSF Secure and Trustworthy Cyberspace (SaTC) community, NSF has funded cybersecurity resources for the NSF community in the form of the Center for Trustworthy Scientific Cyberinfrastructure (CTSC)[3] and the Bro Center of Expertise[4]. Additionally, NSF has funding for applied cybersecurity for science available under the Cybersecurity Innovation for Cyberinfrastructure (CICI)[5] program. These resources provide focal points for aggregating experiences, and translating the work from the broader world into cybersecurity practices effective for NSF scientific computing.

CTSC, now in its third year, reestablished the NSF cybersecurity summits means to reinvigorate

[1] http://www.nist.gov/cyberframework/
[2] http://www.nist.gov/nstic/
[3] http://trustedci.org/
[4] https://www.bro.org/nsf/
[5] http://www.nsf.gov/pubs/2015/nsf15549/nsf15549.htm

the NSF cybersecurity community and increasing out trust of the science supported by that community.. Spanning six years from 2004 to 2009 and then reinstated in 2013, the annual NSF Cybersecurity Summits serve as a valuable part of the process of securing NSF scientific cyberinfrastructure (CI) and increasing our trust in the science it supports by providing a forum for education, sharing experiences, and building community. For many attendees, the summits are unique opportunities to come together with their colleagues, to benchmark and debate cybersecurity best practices, and to receive practical, relevant training.

The 2015 summit took place Monday, August 17th through midday Wednesday, August 19th, at the Westin Arlington Gateway near NSF. On August 17th, the summit offered a full day of training in response the strong training attendance in both 2013 and 2014 and overwhelmingly positive feedback. The second and third days followed a workshop format designed to identify both the key cybersecurity challenges facing Large Facilities and the most effective responses to those challenges. The event brought together leaders in NSF CI and cybersecurity to continue the processes initiated in 2013: building a trusting, collaborative community, and seriously addressing that community's core cybersecurity challenges.

The remainder of this report outlines the summit's organizational process, the resultant program, details on attendance and participation, and results of attendees' evaluations of the event. The report concludes with Recommendations and closing thoughts of the organizers.

2 The Summit's Purpose, Scope, and Theme

The 2015 summit built on the Recommendations of the 2014 summit[6], which was well received both as an educational opportunity and a community networking event. We organizers believe the summits can go even further, and support measurable progress on the following goals: identifying, establishing and sharing community standards for best practices regarding cybersecurity; providing pragmatic levels of information security; meaningfully addressing software assurance, quality or supply chains in the context of the project cybersecurity programs; and supporting scientific discovery.

Two recommendations of the 2014 summit served as overarching drivers for the 2015 event:

> *2014 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

[6] See the 2014 summit report, agenda, and more at http://trustedci.org/2014summit/

particular needs around unique scientific instruments, data, openness, multi-organizational relationships, and project lifespans.

2014 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 stakeholder

As such, we set out the dual purposes of the proposed 2015 summit and anticipated future summits as: (a) to support the development of a trusting, collaborative community; and (b) to substantially address that community's core cybersecurity challenges. For 2015, we determined to focus efforts around the theme, ***Understanding the Information Assets that Enable Science***. Information assets that enable science were a natural focus for 2015, representing a massive investment of national resources which entail the production, maintenance, and use of valuable (and sometimes one-of-a-kind) information systems and data.

3 The Organizing and Program Committees

The 2015 summit was funded by a supplemental grant from NSF to the CTSC project, and five members of that project (Craig Jackson, James Marsteller, Susan Sons, Amy Starzynski Coddens, and Von Welch) along with Leslee Cooper, the Administrative Director for the IU Center for Applied Cybersecurity Research, served as the organizing committee. We recruited a Program Committee (PC) made up of key leaders from NSF CI projects and the broader community. The PC was to be responsible for setting the agenda and inviting speakers, evaluating and selecting from among proposed 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 14 meetings by conference call beginning April 10, 2015 and ending August 21, 2015. It conferred electronically both prior to and following this time period, with monthly meetings commencing in October under the purpose of moving summit preparations to a more continuous flow during the year.

The 2015 PC members were:

- **Steve Barnet,** 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**, Deputy CIO and CISO for Brandeis University.
- **Barbara Fossum**, NEES deputy center director and former managing director of Purdue University's Cyber Center and Computer Research Institute.
- **Ardoth Hassler**, Associate Vice President of University Information Services & Executive Director, Office of Assessment and Decision Support at Georgetown University and former Senior Information Technology Advisor in the Office of the Chief Information Officer in the NSF Office of Information and Resource Management, Division of Information Systems.

4 The Call for Participation and Program

The full agenda and biographies are attached to this report as Appendices A and B[7].

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 and full-day trainings, (c) one to two page abstracts for proposed breakout sessions and miscellaneous activities, or (d) student applications.[8] Additionally, the PC invited specific community leaders as well as experts from outside the community to give presentations and participate in panels.

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 with the addition of "breakout sessions and other activities.", Additionally "Tips for Building CFP Responses" was provided to guide and encourage respondents. The CFP process proved a success, and drove a great deal of the resultant program, including 1 case study presentation, 3 panel topics, and 6 training sessions, as well as keynotes from the cybersecurity community at large, and presentations from key leaders from within the NSF community. A particular highlight to note this year was a marked increase in CPF proposals, many more than we had capacity to accommodate resulting in an even stronger community driven program. Some of the unselected proposals were offered and many accepted to lead a table talk version of their CFP submission.

On August 17th, we offered a full day of training in response to 2013 and 2014's overwhelmingly positive feedback and strong attendance. Descriptions of each training session

[7] The full summit program is also available on the CTSC website, http://trustedci.org/2015summit/

[8] http://trustedci.org/2015-nsf-cfp; see also Appendix C.

are appended as Appendix D.[9]

On August 18th and 19th, the Summit followed a workshop format designed to explore our theme of Understanding the Information Assets that Enable Science and identify other cybersecurity challenges facing the NSF community and t effective responses to those challenges. A highlight of the event included a keynote offered by Dr. George Strawn, former Director of NITRD NCO and former NSF CIO. In addition to the CFP-driven portions of the program, the plenary workshop saw significant contributions from NSF, as well as colleagues from the broader scientific and cybersecurity communities. On August 18, Program Committee members and community members led 5 "table talk" discussions during lunch, and many attendees came together again on their own time for an informal dinner that evening.

5 Participants

As with prior summits, attendance was by invitation only, with free registration. Invitations were inclusive of the NSF CI and Large Facility community and used to manage logistics rather than exclude anyone who wanted to attend. Our invitation list was based on the invitation list from the 2014 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 ensure that NSF cybersecurity evolves to address their needs. Additionally, we invited individuals from outside the NSF community (*e.g.*, Department of Energy, Internet2, higher education) to avoid being insular, maintain and develop new relationships, and encourage infusion of additional perspectives.

One hundred individuals registered for the summit, and 90 attended (including speakers, training presenters, panelists, students and the program committee). A listing of the attendees and their affiliations is in Appendix E. Fifty-two attendees participated in the August 17 training sessions. Fifty-one individuals -- over one half of all registrants -- participated in planning, spoke, provided training, co-authored a CFP submission, and/or led a lunch table talk. Five attendees were students. Fourteen) attendees work at Large Facilities. Eighteen attendees work at the NSF.

The following 50 NSF-funded projects or programs, including 14 Large Facilities (marked with "◆"), were represented at the summit. NSF directorates represented by program officers are marked with "**^**".

[9] See also, http://trustedci.org/2015training/

- ATLAS
- AURA
- BCC-SBE
- Blue Waters
- Bro Center of Expertise
- CC*DNI/CC-NIE or CC*IIE projects (4)
- Center for Trustworthy Scientific Cyberinfrastructure (CTSC)
- Cerro Tololo Interamerican Observatories
- CesrTA
- Conference on Privacy in the Infosphere
- Cornell High Energy Synchrotron Source (CHESS) ♦
- CMS
- Directorate for Computer & Information Science & Engineering - Division of Advanced Cyberinfrastructure**^**
- Directorate for Computer & Information Science & Engineering - Division of Computing and Communication Foundations**^**
- Directorate for Computer & Information Science & Engineering - Division of Computer and Network Systems**^**
- Directorate for Engineering - Division of Civil, Mechanical & Manufacturing Innovation**^**
- Directorate for Mathematics & Physical Sciences - Division of Materials Research**^**
- Directorate for Mathematical & Physical Sciences - Division of Physics**^**
- Directorate for Geosciences - Division of Ocean Sciences**^**
- Directorate for Geosciences - Division of Polar Programs**^**
- Cybercorps: Scholarship for Service
- Developing Applications with Networking Capabilities via End-to-End SDN (DANCES)
- EarthCube - EAGER
- Extreme Science and Engineering Discovery Environment (XSEDE)
- Extreme Science and Engineering Discovery Environment - Kraken Extension
- Extreme Science and Engineering Discovery Environment - TIS
- Flight-Worthy Condor: Enabling Scientific Discovery
- Gemini Observatory ♦
- GENI Engineering Conference
- IceCube South Pole Neutrino Observatory (IceCube) ♦
- International Ocean Discovery Program ♦
- Jetstream
- Laser Interferometer Gravitational-Wave Observatory (LIGO) ♦
- Large Synoptic Survey Telescope (LSST) ♦
- National Center for Atmospheric Research (NCAR) ♦
- National Center for Supercomputing Applications (NCSA)

- National High Magnetic Field Laboratory (Magnet Lab) ♦
- National Optical Astronomy Observatory (NOAO) ♦
- National Radio Astronomy Observatory (NRAO) ♦
- National Solar Observatory (NSO) ♦
- Network for Earthquake Engineering Simulation (NEES) ♦
- NHERI
- NTP Security Project
- Ocean Observatories Initiative (OOI) ♦
- Office of Budget, Finance, and Award Management - Division of Acquisition and Cooperative Support**^**
- Office of the Director**^**
- Open Science Grid (OSG)
- Pittsburgh Supercomputing Center (PSC)
- San Diego Supercomputer Center (SDSC)
- NSF Science Support Office
- SI2-SSI: SciDaaS – Scientific data management as a service
- Stampede (TACC)
- SWAMP (DHS)
- Sustain-GT
- UC Berkeley TRUST REU
- US Antarctic Program **♦^**
- Wrangler (TACC)

In addition to the above professionals, the Summit supported the participation of five outstanding students: Anahita Davoudi, Charles McElroy, Dora Baldwin, Jarylin Hernandez, and Matt Bryson.

Finding 4 from the 2013 summit stated "Future program committees should take on gender, age, and racial/ethnic diversity in the community and summit attendance as a strategic imperative for future summits." The organizers recognize that diverse participation is both a socially relevant outcome for NSF[10] and a particular challenge in the cybersecurity community in general[11]. Thus, in 2014, we expressly addressed the topic with the PC, identifying two members to spearhead efforts (Baylis, Hassler), and the group sought to encourage diverse participation via the invitees, speakers, panelists, and PC itself. Additionally, the CFP expressly

[10] *See*, NSF GPG, Section II.C.2.d.i

[11] *See, e.g.*, *Agents of Change: Women in the Information Security Profession.* A whitepaper derived from the 2013 (ISC)2 Global Information Security Workforce Study. Available from: https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/Women-in-the-Information-Security-Profession-GISWS-Subreport.pdf

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. Baylis and Hassler again spearheaded these efforts in 2015, building on the success seen in 2014.

In order to gather ongoing baseline data related to this diversity effort, 2015 registrants had the option to provide their ethnicity/race and gender/sex. There was a small increase in the number of female registrants in 2015, and no change in the ethnicity/race of registrants. The aggregated responses to the those items follow. Voluntary responses to these questions show:

Ethnicity / Race	
Asian or Southeast Asian	5
Black or African American	3
Hispanic or Latino	4
Native Alaskan or American Indian	0
Multiracial	1
White or Caucasian	63
Other Ethnicity	0
Other (space provided)	0
Prefer not to answer	2
No Answer Provided	12

Gender / Sex	
Female	18
Male	49
No Answer Provided	23

6 Attendee Evaluations

We sought attendee evaluations of the summit via two SurveyMonkey surveys. One survey gathered feedback on the summit generally; the other requested feedback specific to the August 17 training sessions.

6.1 Attendee Survey

A summary of the general survey results is appended to this report as Appendix F. The responses were generally very positive, with responses to Question #13, "How can we improve the summit experience in the future?," seeing attendees requesting slight logistical changes and requesting that CTSC continue what they are doing. One attendee captured this theme with the response "Keep listening and doing the great job of building the community and awareness." Another attendee stated "I think the experience is great. We need to work to maintain the energy and engagement from all parties. I think if we can make sure we emphasize outcomes and highlight the progress that has been made and reinforce that this progress is a direct result of community effort it will help sustain that energy." The program committee has taken this feedback into consideration and will continue to consider it during the planning of the 2016 summit.

A summary of the additional survey responses follows.

Forty-two attendees (approximately 47% of all attendees) responded to the general "Attendee Survey." The organizers did not submit responses, but the survey was open to all other participants. We did not request the names of respondents, and have redacted some information from the appended report to further protect the anonymity of respondents.

The quantified and categorical results (*e.g.*, rating scales, yes/no questions) were very favorable. Selections follow:

- To Question #5, "How would you rate your overall experience with the 2015 summit?," 95% of respondents selected "Good" or "Excellent."

- Regarding Question #7, "Was this summit better than what you expected, worse than what you expected, or about what you expected?," the summit at least met the expectations of 98% of respondents, exceeding the expectations of 79% of respondents.

- To Question #8, "How useful to your work was the information discussed at the summit?" 100% of respondents gave ratings of "moderately useful," "very useful," or "extremely useful," with 79% providing the higher two responses.

- To Question #9, "If you attended last year's summit, how does this year's compare?" 47.62% of respondents gave ratings of "this year's summit was about the same as last year's," "this year's summit was better than last year's," or "this year's summit was much better than last year's," with 33.33% providing the higher two responses. 52.38%

of respondents indicated that they did not attend last year's summit.

- To Question #11, "Would you like to attend future summits?" 85.71% responded "Yes," with the remaining 14.29% responding "Maybe."

Questions 13 and 14 sought open-ended responses, and were designed to elicit critique and discern highly-valued aspects of the experience. While the generally positive results of the above-referenced questions provide context, these open-ended questions have proved a useful communication tool. Observations follow:

- Question 13 asked, "How can we improve the summit experience in the future?"
  - Of the 26 respondents to this question, 6 suggested extending the length of the summit. An example response follows:

    "The summit should have been at least 3 days. There was far too little time for networking and getting to know everyone. Breakfast needs to be much better it is hard to begin your day and think clearly on sugar. I was surprised to learn there was not a dinner night -- food provided with a cash bar. These are usually the best opportunities for group discussion and networking. Having separate meals usually ends up with groups of people that know each other sectioning off which leaves the new folks in a lurch. Have at least one half day of topical focus groups. For instance, have several sections of different types of security: Network, Mobile, Server, Organisation. Underneath those headings anyone can write in a question -- they can then attend those focus groups to have those questions answered as a group rather than a single individual. This is a fantastic way to get people with similar areas of concern together and talking. It also helps each individual glean the expertise of everyone in the group which helps with future collaboration."

- Question 14 asked, "Were there any aspects of the summit you found particularly useful or important? If so, please explain."
  - Of the 22 respondents, 3 praised the panel discussions and 3 highlighted the training sessions as particularly useful or important.
  - Eight (8) respondents highlighted networking opportunities.

6.2 Training Evaluation

The responses to the training-specific surveys were very positive generally, and included constructive feedback, as well as ideas for future training offerings. For simplicity, we asked

attendees to complete one survey with several repeated questions to allow sorting differentiated responses for morning and afternoon sessions. The aggregated ratings in Questions 1 through 10, and 13 through 18 are attached as Appendix G. We summarize a few aggregate responses below:

- To Question 3, "Based on your overall experience with the August 17 training sessions, would you participate in training offered at future summits?," 24 (*i.e.*, 96%) of 25 respondents selected "Yes," 1 selected "Maybe," and 0 selected "No."

- To Questions 7 and 15, "How would you rate your overall experience with the [morning/afternoon] training?," 83% of responses were "Excellent" or "Good."

- To Questions 9 and 17, "Was this [morning/afternoon] training better than what you expected, worse than what you expected, or about what you expected?," 94% of responses indicated that expectations were met or exceeded. Forty-one (41%) of responses were "Quite a bit better" or "A great deal better."

- To Questions 10 and 18, "How useful to your work was this [morning/afternoon] training?," 73.5% of responses were "Very Useful" or "Extremely Useful."

The responses for the individual trainings were reported back to their respective training leaders, including responses to Questions 11 and 19, "How can we improve this training session in the future?" and Questions 12 and 20, "Were there any aspects of [morning/afternoon] training you found particularly useful or important? Please explain."

7 Recommendations and Supporting Discussions

In open discussion during the summit's plenary, Cliff Jacobs asked the audience for a show of hands: *Has information security gotten easier or more difficult for NSF projects and facilities in recent years?* A sizeable majority raised their hands for *more challenging*.

When asked if we've made progress as a community on our security posture, again there was strong agreement: *Yes, we have, but not as much as we'd like.*

The 2015 summit evidenced greater maturity and detail of discourse, as well marked progress on recommendations from the prior year's report. At the same time, the discussions and feedback on the event highlighted newly unearthed, pressing issues; established some activities as standing action items; raised awareness of new opportunities; and identified open questions simply requiring more exploration. The following subsections make recommendations regarding Priority Recommendations (7.1), Recommendations for Continued Action (7.2), and

Opportunities and Recommendations for Exploration (7.3). Each recommendation is followed by a discussion of supporting evidence.

7.1 Priority Recommendations

Facilitated by the Call for Participation and increased in-depth, open sharing, the 2015 summit identified three areas in need of focused attention to ensure that projects and facilities have sufficient resources, information security governance structure, and positions on software assurance requirements to make effective information security programs a reasonable possibility.

7.1.1 Information Security Budgets

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.

*Discussion***:**
This year, project and facility budgets for information security emerged as a major theme and major question. George Strawn's keynote emphasized that the balancing act of how much to spend on security will always be with us. Cliff Jacobs' retrospective look at this community's history with information security described scientists asking him, 'which part of the science to give up' in order to do information security.

Several discussions, including Strawn's keynote and the *Anatomy of a Data Breach* panel made absolutely clear that this community has experienced and continues to experience significant mission-impacting information security incidents. However, it remains unclear whether and how much spending should increase to reduce the potential for future losses of availability of scientific facilities and integrity and appropriate confidentiality of scientific and administrative data. Ongoing frank, focused discussions that include bother cybersecurity practitioners and stakeholders areneeded to arrive at an appropriate funding strategy.

7.1.2 Accountability, Risk Acceptance, and the Role of Project Leadership

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.

Discussion:
2014's Finding C stated, Cybersecurity is a "whole-of-organization" endeavor, requiring input and buy-in both vertically (from PI's and directors to staff and users) and horizontally (*e.g.*, scientists, legal, IT, HR) across project organizations, and coordination with cooperating, hosting research institutions. This finding and supporting discussion led to two recommendations:

> ***2014 Recommendation 3****: The NSF CI and Large Facility community should identify and share best practices for how to successfully integrate security throughout project organizations.*
>
> ***2014 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.*

The role of project leadership emerged as a theme across many discussions. George Strawn's keynote highlighted how high level executives are increasingly being held accountable for major information security breaches, citing the recent OPM breach as an example. The *Anatomy of a Data Breach* panel and related discussion not only raised concerns about NSF project leadership's understanding and support for information security, but explored methods for effective communication up the chain of command. Tim Howard's discussion of executive awareness explored similar ground.

The 2015 summit did provide a significant platform for sharing best practices for information security integration throughout the organization. Alex Wither's talk on LSST's information security program was a prime example, explicitly addressing LSST's processes for information security risk acceptance, and the assignment of risk responsibility and ownership. However, the summit itself has seen relatively little and certainly inconsistent attendance by high level project leadership or PIs, with some notable exceptions. As such, it is hard to say whether those key stakeholders have really had a voice in this venue.

As such the latter 2014 recommendation is expanded to emphasize the importance of stakeholder involvement, including project leadership, and highlights the need for an understanding of not only risk responsibility and acceptance processes, but ultimate accountability.

7.1.3 Requirements for Software Assurance, Quality, and Supply Chain

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

Discussion:
Per 2014 Recommendation 7C[12], this year's summit featured talks by Dave Nalley, *The Tragedy of Open Source,* and Amar Takhar, *Risks of Infrastructure Neglect and the Road Ahead*, focusing a detailed discussion on challenges to open source software maintenance as they pertain to security. In particular these talks noted the lack of security resources for key software in the supply chains of NSF projects and recent major vulnerabilities in that software e.g. Heartbleed, Shellshock). The session was very well-received and well-reviewed in the Attendee Survey as an eye-opening presentation, and inspired recommendations to continue the discussion at future events, perhaps expanding to focus on commercial software. Attendee questions and comments make clear that a common understanding of the community's software assurance, quality, and supply chain requirements is urgently needed.

7.2 Recommendations for Continued Action

The 2015 summit highlighted a handful of areas for continued work, most identified in prior years' findings and recommendations. These are areas where there is evidence that progress is being made, but must continue. Though not as urgent as the issues in Section 7.1, they are just as important and foundational for the community's continued maturation with respect to information security.

7.2.1 Baseline Expectations

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.[13]

*Discussion***:**
Presenters and trainers discussed a variety of sources of best practices and baseline security

[12] "For each of the following open questions, 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 ... 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?"
[13] This is a revision of 2014's Recommendation 1: "The NSF CI and Large Facility community should define its own best practices for cybersecurity rather than expecting them to be directed to them from NSF. Clearly setting our own standards will help protect us from compliance directives not as well-suited to our community."

expectations, including CTSC's *Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects*[14], FISMA / NIST Special Publications, HIPAA, and the SANS Critical Security Controls. There is an increasing awareness of the range of available resources. However, no framework has emerged as dominant or preferred. This year's event included very little discussion of evaluative metrics.

It is clear that NSF-funded facilities and projects understand that they are responsible for defining their own information security programs. One respondent to the Attendee Survey stated the following in response to Question 9, *If you attended last year's summit, how does this year's compare?*:

> "Community seems to be coming together. Good, direct communicating. Community contribution needs to drive this and it looks like this is the case. I was happy to hear less of "why doesn't NSF tell us what to do" sort of questions. I think that indicates that the community has at some level come to grips with this and understands how to proceed."

However, the assumption that NSF should play little role in setting baseline expectations was directly called into question during the *Anatomy of a Data Breach* panel by NSF CIO Amy Northcutt. As discussed in Section 7.1, that panel and other discussions highlighted some ways in which NSF projects and facilities may have insufficient resources, incentives, or leadership buy-in to adopt and implement uniform or effective baseline security expectations.

A focused effort to adopt a common framework, including risk management processes, best practices, resources, and evaluative metrics would be useful for facilitating community dialogue, developing a more cohesive community of practice, and improving the community's collective security posture.

7.2.2 Risk-Based Approaches

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.[15]

[14] trustedci.org/guide

[15] This is a revision of 2014's Recommendation 2: "The NSF CI and Large Facility community should continue to strive toward a risk-based approach to cybersecurity that leverages broader best practices as much as possible, while also addressing the community's particular needs around unique scientific instruments, data, openness, multi-organizational relationships, and project lifespans."

Discussion:
Risk-based approaches to information security were discussed throughout the 2015 event and, consistent with the general societal trend, have at least rough consensus as the appropriate approach for the community. Both plenary discussion and the evaluation surveys saw suggestions that the plenary might include more specific presentations regarding risk processes (*e.g.*, how to do risk assessments) that have been contained largely within training sessions for the past two years. The summit's asset-focused theme resonated in both Kent Wada's and Tim Howard's talks, highlighting the importance and challenges of documenting the nature and location of information assets within risk-based approaches. Wada's talk highlighted the importance of mission, emphasizing that risk-based approaches should not lose sight of the organizational mission when tackling risks. George Strawn's talk, Tim Howard's talk, as well as Anurag Shankar's comment in open discussion, introduced the increasingly popular "resilience" concept to the discussion.

7.2.3 Community Building & Information Sharing

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.[16]

Discussion:
This summit marked a dramatic increase in the open discussion of projects' and facilities' specific information security practices and lessons learned, with CFP responses driving the majority of the agenda. The open-ended questions and optional comments to the Attendee Survey were replete with praise for this openness and the community-driven nature of the content, and also included several calls for even more sharing. When asked, "What presentation format(s) did you find most valuable? (You may select more than one.)," Attendee Survey respondents gave the plenary case studies (*e.g.*, Alex Wither's LSST talk) the most marks.

The community should continue the level of sharing and collaboration emerging at the summit, but needs to do more outside the summit itself. In general, there was little evidence presented at the summit that sharing of information security best practices occurs among NSF projects and facilities outside of the annual summits. Particularly because the utility and availability of usable threat intelligence and information sharing services is in question (see below, Section

[16] This is a revision of 2014's Recommendation 5: "The NSF CI and Large Facility community should explore ways of collaboratively developing and maintaining cybersecurity programs, such as sharing materials, services, practices, lessons learned, and collaborative/peer reviews."

7.3.3), the community should build on what is happening at the summits and create more opportunities for peer-to-peer and direct community sharing of best practices.

When asked for a show of hands, plenary participants overwhelmingly indicated that they would be willing to participate in an anonymized community survey to gather community-wide information on threats, incidents, and/or security program status.

Romain Wartel emphasized the particularly strong need and possibilities for coordination and sharing among the R&E community. Alex Withers emphasized XSEDE as an example of positive resource sharing, and highlighted the importance of the CISO's contact list in effective information security. In open discussion and in the Attendee Survey responses, community members cited the value of bringing the international science community into the discussion.

7.2.4 Identity and Access Management

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.

Discussion:
In spite of the fact that identity and access management (IAM) received very little explicit billing in this year's program agenda, IAM's importance for enabling and securing science came up repeatedly. Bill Miller discussed the need for identity management to evolve to handle the increasing complexity of scientific workflows. Both Alex Withers and Tim Howard discussed how access and access control are critical to enabling their respective facilities' science work. Moreover, there were some implicit indications that community members are not uniformly aware of the solid IAM resources already available to the science community. When asked how we can improve future summits, an Attendee Survey respondent suggested, "...consider a stronger focus on identity management since both NCAR and LSST found it a major part of their challenge."

Additionally, on the first day of plenary, nine summit attendees actively participated in a lively and productive table discussion on the topic of federated identity needs that covered topics including international interfederation, incident response, offboarding campus accounts, certificates and non-web access, attribute release, and technical approaches (Grouper, COmanage). All agreed that identity management continues to be a pain point for managing secure access to cyberinfrastructure and, in particular, that there is a need for educational materials and training for campuses on attribute release to support scientific collaborations. When identity management for cyberinfrastructure is neglected, scientists are inconvenienced and the risk of inappropriate access to campus resources grows. Campus identity management

systems, federated through InCommon, can significantly ease this pain point for cyberinfrastructure operators.

While the definitions of and relationships among identity management (IdM), IAM, and information security vary across communities and organizations, it is beyond question that they are intertwined in effect. IAM has enormous implications for information security in every environment, and perhaps particularly so for the R&E community. This recommendation serves to acknowledge this critical facet of the information security landscape.

7.2.5 Privacy

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.

Discussion:
Per 2014 Recommendation 7B[17], this year's summit included a privacy-oriented talk by UCLA Chief Privacy Officer Kent Wada, as well as a panel entitled *Privacy and Big Data: A New Frontier for Research Cyberinfrastructure*. Notably, both sessions focused a great deal of discussion on organizational process and mission. Wada's talk contextualized privacy and regulatory issues in the context of organization mission. Jeff Collman's contribution centered on the need to break down intra-organizational silos to enable organizations to tackle multi-faceted issues like privacy. There was no indication that the community has directly taken up a research effort. However, respondents to the Attendee Survey encouraged the summit to continue addressing privacy.

7.3 Opportunities and Recommendations for Exploration

The 2015 summit identified new areas of opportunity, as well as areas identified in prior years' findings and recommendations that remain open questions. The recommendations focus on areas for exploration to identify the magnitude or benefit or risk associated with each area.

7.3.1 NSF-Funding Facilities and Projects as Real-World Cybersecurity Research Environments

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

[17] "For each of the following open questions, 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. . . . 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?"

that funded via NSF's Secure and Trustworthy Cyberspace (SaTC) and Risk and Resilience solicitations.

Discussion:
Several talks and panels returned to a common theme: Cybersecurity is so challenging because cybersecurity problems are so very human. In discussing the nascent "science of cybersecurity" and transition to practice, George Strawn emphasized this human factor as a potential barrier to progress, arguing we cannot have a science of security without the behavioral and organizational sciences. NSF's Anita Nikolich explicitly suggested that NSF-funded facilities could be real-world research environments where cybersecurity researchers could do meaningful *in situ* research, simultaneously building a rich, evidence-based science of cybersecurity as well as benefitting the participant projects and facilities with greater insight into their own security operations and cutting edge findings. Research opportunities can also act as a vehicle to advance cybersecurity skillsets of staff, promote a culture of cybersecurity within an organization, assist with transitioning research to practice, and advance existing cybersecurity efforts.

7.3.2 Community Threat Model

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.

Discussion:
Per 2014 Recommendation 7A[18], the NSF Cybersecurity Center of Excellence (CCoE)[19] will be tasked with "[d]evelop[ing] a threat model (or multiple threat models if appropriate), identifying the vulnerabilities in NSF-funded cyberinfrastructure and scientific data associated with that cyberinfrastructure and recommending countermeasures to protect the systems." Von Welch highlighted this new initiative and impact from prior summits in his talk, *Trustworthy Computational Science*. As the direct audience for this work, the community has a role to play beyond simply choosing to utilize or or not utilize the ultimate product of that effort.

---

[18] "For each of the following open questions, 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 . . . 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?"

[19] See, NSF 15-549 (Program Solicitation), Cybersecurity Innovation for Cyberinfrastructure (CICI). Available at http://www.nsf.gov/pubs/2015/nsf15549/nsf15549.htm

7.3.3 Real Time Data, Threat Intelligence, and Information Sharing Services

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.[20]

Discussion:
There is little indication that projects or facilities have found ways to share real-time data or make use of existing cross-organizational mechanisms. REN-ISAC came up explicitly, but it remains unclear whether that organization will evolve to better support the NSF science community. It remains to be seen whether and to what extent the community will make use of information sharing to bolster information security.

8 Closing Thoughts from the Organizers

The summit is making noticeable strides both in building community and tackling the challenges of cybersecurity in the context of NSF science. The discussions among participants are becoming more open and more nuanced, with identification of the lack of a clear cybersecurity budget strategy as a key challenge this year. In past years, nuanced discussions of a non-technical nature were rare. The community also seems to be reaching at least rough consensus on risk-based approaches to cybersecurity.

It was great having the energy and enthusiasm of the student scholars at the Summit. We look forward to continuing this development of a new, inclusive workforce next year.

We're excited about the NSF solicitation which includes a Cybersecurity Center of Excellence which will continue these Summits. We believe this will not only continue these summits but foster year-around activity from this community.

We thank all the participants for their contributions, particularly those who responded to the call for participation. We especially thank the participants who shared their experiences and lessons learned from incident response. We believe this type of sharing is essential for building a meaningful community of cybersecurity practice.

Finally, we thank the program committee members for their hard work and devotion to the

[20] This is a revision of 2014's 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 as well as gain as much of an advantage as possible with regard to defending ourselves. Existing cross-organizational mechanisms (*e.g.*, REN-ISAC, EDUCAUSE, Internet2) should be considered here in terms of how they could be leveraged."

summit, and we thank NSF for funding and providing presentations.

The 2015 summit was very well-received, and we believe the event fulfilled the dual purposes set out in the early planning stages: (a) to support the development of a trusting, collaborative community; and (b) to substantially address that community's core cybersecurity challenges. We again thank the Program Committee and all who responded to the CFP, spoke, provided training, and actively participated, for making the 2015 summit a success.

As organizers, our goal has been to push the summits to maximize their positive impact on cybersecurity for the NSF CI and Large Facility community, and we believe 2015 saw a number of improvements over the 2013 and 2014 events. With the success of the CFP process, the program was more community-driven, and the program was even more deeply substantive than in previous years. The discussions benefitted a great deal from the presence of, strong participation from, and frank discussions with NSF program officers and personnel. The summit brought together many attendees, projects, and facilities, allowing for community engagement and depth that have supported the drafting and vetting of a more detailed set of Findings and Recommendations. For CTSC, the summit was once again a forum for forming new relationships and an opportunity to plan new engagements, as well as a chance to socialize CTSC's *Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects*.[21] Our attendee surveys showed overwhelmingly positive evaluations of the event, as well as thoughtful critique and new ideas.

One of the most encouraging -- and yet most challenging -- things we observe is a strong desire in the community for more opportunities to share materials, services, practices, and lessons learned. We note that the Summit is part of NSF's Cybersecurity Innovation for Cyberinfrastructure (CICI) solicitation[22] and these valuable events will continue as part of NSF's Cybersecurity Center of Excellence. We suggest the new center plan to continue address the community's continued desire for sharing in the 2016 summit, as well as consider how it can support these activities between the summits. CTSC is working with the REN-ISAC and other members of the community to determine more precisely what content, format, and fora will best meet the community needs, including increased opportunities for these types of interactions at the summit itself.

Diversity in attendance, community-driven cybersecurity program development, and addressing 2013 concerns became a strategic item for the PC for 2014, then again in 2015. The

[21] http://trustedci.org/guide

[22] http://www.nsf.gov/pubs/2015/nsf15549/nsf15549.htm

2015 summit was a great improvement over 2013 in terms of gender and age inclusiveness, in part due to the PC's focused effort and in part due to attendance by and participation from NSF personnel. There was not much change in the demographic data around attendees from 2014 to 2015, but we are determined to continue efforts to appropriately encourage diversity / inclusion in future summits, determine appropriate process and outcome metrics for this effort, and leverage the baseline data we collected as factual background for future discussions.

We suggest the 2016 summit continue the successful process of program building by convening a program committee and issuing a call for participation. We hope to see even more of the agenda driven by community submissions. The focus of the 2016 summit will be addressing the 2015 Recommendations and documenting Large Facilities community progress. A secondary focus will be maximizing the positive impact on the broader scientific CI ecosystem by considering how Large Facility practices relate to medium-sized projects.

Appendix A
The Agenda

Program Agenda

2015 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure

August 17 - August 19 Westin Arlington Gateway Arlington, Virginia

http://trustedci.org/2015summit/

Updated August 14, 2015

Program Committee: Steve Barnet, Tony Baylis, Mike Corn, Barb Fossum, Ardoth Hassler
Organizers: Amy Starzynski Coddens, Leslee Cooper, Craig Jackson, James Marsteller, Susan Sons, Von Welch

---

Training Day

Monday, August 17, 2015

http://trustedci.org/2015training/

7:00am	Registration and Continental Breakfast (Hemingway Pre-Function)
8:00am	Morning and All Day Training Sessions Begin ● Bro Platform Training Workshop ● Developing Cybersecurity Programs for NSF Projects ● Vulnerabilities, Threats, and Secure Coding Practices ● Industrial Control Systems, Networking, and Cybersecurity
10:00am	*Coffee Break*
10:30am	Training Sessions Resume
12:00pm	*Lunch provided*
1:00pm	Afternoon Training Sessions Begin and All Day Training Sessions Resume ● Bro Platform Training Workshop (continued) ● Developing Cybersecurity Programs for NSF Projects (continued) ● Aligning your Research Cyberinfrastructure with HIPAA and FISMA ● Incident Response Training
3:00pm	*Coffee Break*
3:30pm	Training Sessions Resume
5:00pm	Sessions End
Evening:	*Dinner on your own*

Plenary Session

Tuesday, August 18, 2015
F. Scott Fitzgerald C

7:00am	Sign-In and Continental Breakfast (Pre-Function AB)
8:00am	Welcome and Goals (Jim Marsteller)
8:10am	NSF Address: Bill Miller, Science Advisor, Division of Advanced Cyberinfrastructure (ACI)
8:30am	Keynote Address: George Strawn, "Science or Security"
9:30am	A historical perspective on addressing cyber-security in NSF supported communities (Cliff Jacobs)
10:00am	*Coffee Break*
10:30am	Trustworthy Computational Science (Von Welch)
11:00am	Case Study: Cyber Security Challenges Facing the Large Synoptic Survey Telescope (Alexander Withers)
11:45am	Lunch and Table Topics - *Lunch provided*
1:15pm	Panel: "The Anatomy of a Data Breach" Moderator: Amy Northcutt, NSF CIO Panelists: Susan Ramsey (UCAR) Karen Stocks, PhD (Scripps Institution of Oceanography) Scott Sakai (SDSC)
2:15pm	*Coffee Break*
2:45pm	Dealing with Cyberthreats: A European Perspective (Romain Wartel, Liviu Valsan)
3:30pm	Beyond Security and Privacy: Trust and the Value of Data (Kent Wada)
4:30pm	Open Discussion / Summary of the Day's Findings (Von Welch, Craig Jackson, Jim Marsteller)
5:00pm	*Adjourn for the Day*
Evening:	*Dinner on your own.* *Informal Dinner Gathering at World of Beer, 901 N. Glebe Rd., 6:30pm*

Plenary Session (continued)

Wednesday, August 19, 2015
F. Scott Fitzgerald C

7:00am	Sign-In and Continental Breakfast (Pre-Function AB)
7:50am	Welcome Back (Jim Marsteller)
8:00am	"Privacy and Big Data: A New Frontier for Research Cyberinfrastructure" Jeffrey Collman, Georgetown University Doug Richardson, Association of American Geographers Moderator: Ardoth Hassler
9:00am	Risks of Infrastructure Neglect and the Road Ahead (Dave Nalley, Amar Takhar)
10:00am	*Coffee Break*
10:30am	"Understanding the Information Assets that Enable Science: Some Thoughts about Operational - Technologies and the Internet of Things in Antarctica" (Tim Howard, National Science Foundation)
11:30am	Open Discussion / Summary of Summit Findings (Von Welch, Craig Jackson, Jim Marsteller)
12:00pm	Adjourn

Appendix B
Biographies for Speakers, Program Committee, and Organizers

2015 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure

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

---

In alphabetical order by surname

Johanna Amann joined the International Computer Science Institute (ICSI) in September 2011, and has been a member of the Bro team since that time. She has worked on quite a few aspects of Bro, including the Input Framework, reworking the SSL/TLS support of Bro and, most recently, on enabling Bro to be able to support software defined networking. Before joining ICSI, she did her PhD as well as her Diploma (Masters equivalent) at the Technical University of Munich in Germany.

*

Security Engineer **Justin Azoff** is responsible for implementing security plans; assisting other NCSA groups in hardening and protecting their systems; and developing, administering and utilizing NCSA's state-of-the-art cybersecurity monitoring infrastructure in support of the Center's objective of providing a highly reliable and functional computing environment. Working with other Security Engineers, Azoff identifies and investigates cybersecurity incidents across NCSA networks and systems and responds to these events, interdicting malicious behavior, mitigating security vulnerabilities, remediating compromised systems and adjusting cybersecurity controls as appropriate to ensure similar malicious behavior is prevented in the future. Azoff has been a Bro user since 2009 and became a Bro developer as part of his security engineer role when he joined NCSA in 2013.

*

Dora Baldwin is a graduate student of California State University, San Bernardino where she is pursuing her Masters of Public Administration with a concentration in Cyber Security. She is a first year recipient of the CyberCorps: Scholarship for Service which is an academic program funded by the National Science Foundation and co-sponsored by the Department of Homeland Security. After graduation, she aspires to work for the federal government and specialize in cyber security oversight and development.

*

Steve Barnet has specialized in supporting scientific and academic computing for nearly 20 years. During that time, he has worked in multiple domains including storage, networking, high-throughput computing, and security. He handled his first incident in 1995, a compromised Solaris system providing several important infrastructure services.

Steve is currently works for the IceCube project, a kilometer scale neutrino detector located at the geographic South Pole. He began collaborating with CTSC in 2013 to develop a Cybersecurity plan for the IceCube facility.

*

Jim Basney is a senior research scientist at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign. Jim leads the CILogon project

(www.cilogon.org), which enables federated authentication to cyberinfrastructure. Jim is also the security technical lead for XSEDE (www.xsede.org) Software Development and Integration (SD&I), and Jim is the identity management lead for the Software Assurance Marketplace (SWAMP). Jim maintains the MyProxy credential management software, an "exemplar of success in cyberinfrastructure software sustainability" according to the report from the NSF workshop on CyberInfrastructure Software Sustainability and Reusability (http://hdl.handle.net/2022/6701). Jim is an active participant in The Americas Grid Policy Management Authority and the InCommon Technical Advisory Committee. Jim received his PhD in computer sciences from the University of Wisconsin-Madison where he worked as a graduate research assistant on the Condor project.

*

Tony Baylis of Lawrence Livermore National Laboratory is the Laboratory's Director for the Office of Strategic Diversity and Inclusion Programs. In this position, he is the senior management advocate for diversity and inclusion for the Laboratory. The Office of Strategic Diversity and Inclusion Programs partners with senior management to develop strategies, initiatives, programs, and activities that promote the creation of a diverse and inclusive workforce and work environment. Tony serves as the Laboratory's EEO, AA and Diversity compliance officer as well. In conjunction with these tasks, 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 26 years of administrative, project, program, technical and organizational management. He has worked in a scientific and technical environment for over 20 years and has worked as an 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 serves on a number of conference program committees and advisory boards that promote STEM and diversity in science and technical careers. He has been an NSF reviewer and PI/Co-Pi for the Broadening Participation in Computing Program. Tony is also an ACM and ACM SIGGRAPH member, and serves as the Treasurer for ACM SIGGRAPH. He is a graduate of the University of Illinois.

*

Matt Bryson is a senior majoring in Computer Science and minoring in Mathematics at California Lutheran University. He currently is working as part of the Computational Research Department at the Lawrence Berkeley National Lab as part of the UC Berkeley TRUST REU program. His research is focused on burst buffer applications, especially concerning exascale computing. He hopes to go on to a PhD in Computer Science, with an emphasis on systems.

*

Randal Butler serves as Deputy Director for CTSC and focuses his expertise within the project on engagements and training. He is the director for NCSA's Integrated CyberInfrastructure (ICI) Directorate that is responsible for the management and oversight of all of NCSA's CI initiatives. ICI has roughly 115 technology focused staff that cover the range of R&D to operations across, systems, data, software & applications, cybersecurity, networking, and information technology. Butler is the former director for NCSA's Cybersecurity Division which is responsible for all NCSA cybersecurity operations

and also includes a nationally recognized team of cybersecurity researchers working in the applied space. He has been PI and co-PI on numerous NSF security focused awards, and he co-led Security Operations for XSEDE, as well as having been involved in a number of national-scale science CI initiatives.

*

Jeff Collmann obtained his Ph.D in Social Anthropology from the University of Adelaide, South Australia, and completed a postdoctoral fellowship in medical ethics at the University of Tennessee. His research focuses on understanding the effect of bureaucracy and other complex forms of organization on everyday life. The results of his research on social change among Australian Aborigines have been published in numerous articles and as a book, Fringedwellers and Welfare: the Aboriginal response to bureaucracy. He joined Georgetown University in January 1992 where he developed a national reputation in the area of ensuring organizational compliance with health information security regulations, including work on the HIPAA security program for the Military Health System. He received the National Intelligence Medallion for helping develop a novel approach to biosurveillance. He has taught the anthropology of Australian culture, biodefense and infectious disease at Georgetown. He was promoted to the rank of Research Professor in the Department of Microbiology in Fall 2011. He currently serves as Director of Use Case Development for the AvesTerra Project, a “Big Data” project sponsored by the Office of the Senior Vice President for Research.

*

Michael Corn is the Deputy CIO and CISO for Brandeis University. His areas of interest include privacy, identity management, and cloud services. He has been an active speaker and author on security and privacy and has participated in numerous Educause and Internet2 initiatives. He is a member of the Internet2 Netplus Product Advisory Board and until recently was also a member of the Box.com and Splunk Product Advisory Boards, as well as the Kuali Ready Product Board.

Prior to joining Brandeis he was the CISO and Chief Privacy and Security Officer of the University of Illinois at Urbana-Champaign. He is a graduate of the University of Colorado at Boulder and the University of Illinois at Urbana-Champaign.

*

Robert (Bob) Cowles is principal in BrightLite Information Security performing cybersecurity assessments and consulting in research and education about information security and identity management. He served as CISO at SLAC National Accelerator Laboratory (1997-2012); participated in security policy development for LHC Computing Grid (2001-2008); and was an instructor at University of Hong Kong in information security (2000-2003).

*

Anahita Davoudi has a Master in Computer science from North Carolina State University (2011), a Master in Electrical Engineering from University of Texas at Arlington (2012), and a Master in Data Mining from University of Central Florida (2016). She is a PhD student at computer science department at University of Central Florida. Her research interests are in Social Network trust modeling and recommender systems. She works on social network trust evolution and online trust relationships.

Before joining the PhD program, Anahita was a master student at University of Texas Arlington

where as part of her master thesis she was working on Salsa (a Structured Approach to Large-Scale Anonymity). Anahita Has been a research assistant at North Carolina State University during her master. She worked on cloud computing and service level agreement.

*

Barbara Fossum is the Deputy Director for the George E. Brown, Jr. Network for Earthquake Engineering Simulations (NEES), at Purdue University in Lafayette, Indiana. In this capacity, Barbara directs the day-to-day operation and the development of cyberinfrastructure to support the $105 million NSF distributed network of 14 earthquake engineering research centers. Barbara came to Purdue from the NSF where she was a Program Manager from 2001 to 2004, for the Information Technology Research initiative within the Office of Cyberinfrastructure Research. While currently devoting her time to Large Facility operations and management, she continues to be engaged in supercomputing activities and scientific visualization.

*

Ardoth Hassler is Associate Vice President of University Information Services at Georgetown University. Her work focuses on policy, planning and research, including being the PI for an NSF CC-NIE award. In addition, she is Acting Director of the Student Information Systems group. Ardoth was on loan to the National Science Foundation 2007-2011 where she served as Senior Information Technology Advisor in the Office of the Chief Information Officer in the NSF Office of Information and Resource Management, Division of Information Systems. Her activities included work related to cybersecurity best practices for large research facilities, working on technology policy for the Foundation and large research facilities, assisting NSF in joining the InCommon Federation and introducing concepts of single-sign-on logon to Research.gov, leading the SSN Be Gone project to remove SSNs from FastLane and other systems where there was no business need, working on NSF's Got Green initiative, etc. She has prior experience serving on the program committees of the NSF Cybersecurity Summit, EDUCAUSE Annual Conferences, etc. She has a BS in Math (CS minor) from Oklahoma State University and an MS in Biostatistics from the University of Oklahoma.

*

Jarilyn Hernandez is a fifth year doctoral student in Computer Science at the West Virginia College of Engineering and Mineral Resources. She participated in DC3 and her team won in the overall worldwide graduate division. She received her BS in Computer Science from the University of Puerto Rico Arecibo Campus. As an undergraduate student she had the opportunity to participate in a summer internship at the University of Science and Technology and Missouri, where she works in the development of a robot that could measure the signal strength indoors. Also she was awarded with the SMART scholarship for two years.

She also has a Masters Degree in Computer Science from the Polytechnic University of Puerto Rico. As a master student she received for two years the National Science Foundation scholarship, and she received a fellowship called Nuclear Education Fellowship Program in which she was working as research and teacher assistant. She also served as an intern at Oak Ridge National Laboratory, where she worked with Dr. Line Pouchard from the Computer Science and Math Division in high performance computing.

Her research interests are cyber security, computer forensics, and human computer interaction. In her free time, she enjoys exploring new places, watching anime and movies. Once she has completed the PhD her goals are to do a postdoctoral at Oak Ridge National Laboratory, and be part of the faculty in

a University in the United States.

*

Elisa Heymann is 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.

She is also in charge of the Security group at the UAB, and participated in two major Grid European Projects: EGI-InSPIRE and European Middleware Initiative (EMI). Heymann's research interests include security and resource management for Grid and Cloud environments, and cyber-security in transportation. Currently she is at the University of Wisconsin working for the CTSC project. Her research is supported by 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.

*

Tim Howard, National Science Foundation, Division of Polar Programs - USAP Information Security Manager

*

Craig Jackson is Senior Policy Analyst at Indiana University's Center for Applied Cybersecurity Research (CACR), where his research interests include risk management, information security program development and governance, legal and regulatory regimes impact on information security, and identity management. He leads engagements and authors guidance for the Center for Trustworthy Scientific Cyberinfrastructure (CTSC); he is policy lead of the security team for the DHS-funded Software Assurance Marketplace (SWAMP); and he is part of the DOE-funded XSIM (Extreme Scale Identity Management) project. He is a graduate of the IU Maurer School of Law (J.D.'10) and IU School of Education (M.S.'04). As a member of the Indiana bar, Mr. Jackson has represented government and corporate clients in constitutional and tort claims. His research, design, and project management background includes work at IU School of Education's Center for Research on Learning and Technology and Washington University in St. Louis School of Medicine. He is a member of Phi Beta Kappa, and was a Lien Honorary Scholar at Washington University in St. Louis.

*

Dr. Clifford A. Jacobs worked for the National Science Foundation (NSF) for 30 years and for 25 years of that time provided oversight to the National Center for Atmospheric Research (NCAR) and its managing organization University Corporation for Atmospheric Research (UCAR). His oversight responsibilities cover a wide range of topics including world class science activities at NCAR, observational research and supporting infrastructure, modeling of climate and weather, use of real-time weather and environmental data for research and education (Unidata), and the development and use of cyberinfrastructure by the scientific community. He worked for the Division of Atmospheric and Geospace Sciences, Geoscience Directorate office, the Office of Polar Programs (now the Division of Polar Programs) and the Division of Advanced Cyberinfrastructure. His experiences also extend to collaborative activities among Federal agencies, participation in the working group to develop NSF clarification of its data policy, the development of requirement for a data management plan, help initiate the EarthCube program, and chaired an internal group of

cyberinfrastructure for NSF-sponsored large facilities. Currently, Dr. Jacobs is consulting through Clifford A. Jacobs Consulting, LLC.

*

Scott Koranda, PhD, specializes on identity management architecture for research organizations. Since 2008, Scott Koranda has designed, deployed, and supported production SAML infrastructures including both the Shibboleth Identity Provider (IdP) and Service Provider (SP) software, for the research and education sectors.

A member of the Laser Interferometer Gravitational-Wave Observatory (LIGO) collaboration for over 10 years, Scott has served as the lead architect for the LIGO Identity and Access Management project since 2007. He was co-principal investigator on the NSF grant that funds COmanage development, and is co-principal investigator for the Center for Trustworthy Scientific Cyberinfrastructure (CTSC).

*

James A. Marsteller, Jr. (CISSP) is the Chief Information Security Officer of the Pittsburgh Supercomputing Center,where he is responsible for ensuring the availability and integrity of the PSC's high performance computing assets. Jim has over 16 years experience in the information security field and more than 25 years of professional experience in the field of technology. Prior to working at PSC, he was a program manager for the Carnegie Mellon Research Institute that provided information security consulting services for government agencies and Fortune 500 companies. Jim leads the XSEDE Incident Response team and is XSEDE's security officer. He is a Co-PI for the Center for Trustworthy Scientific Cyberinfrastructure (CTSC). Jim chaired the program committee for the three most recent past summits, 2009, 2013, and 2014.

*

Charles McElroy is a PhD student in Information Systems at Case Western Reserve University in Cleveland, OH. Currently, I am working on a research project related to the NSF Earth Cube initiative which supports the development of cyber-infrastructure for the Geo-sciences. My thesis work is focused on how scientists from disparate disciplines utilize cyber-infrastructure to coordinate their work when they may have little in common. Included in this study is an examination of how cyber-infrastructure can be designed to promote security protection while meeting the needs of the scientists who utilize it.

*

Barton Miller is Professor of Computer Sciences at the University of Wisconsin. He is Chief Scientist for the DHS Software Assurance Marketplace research facility. He co-directs 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, parallel and distributed program measurement and debugging, and mobile computing. 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 is an active participant in the European Union APART performance tools initiative.

Miller received his Ph.D. degree in Computer Science from the University of California, Berkeley in 1984. He is a Fellow of the ACM.

*

William (Bill) Miller is the Science Advisor for the Division of Advanced Cyberinfrastructure (ACI) in the Computer Information Science and Engineering (CISE) Directorate at the National Science Foundation. ACI sponsors supercomputing resources, advancements in campus and international networking, and major software, data and cybersecurity platforms and tools, for the nation's research community. Bill's focus is on forging new integrative activities and partnerships on science-driven cyberinfrastructure within NSF and with external domestic and international entities. He has also been closely involved in policy, planning and oversight of NSF large facilities; and serves in leadership roles for NSF's participation in federal neuroscience efforts including the President's BRAIN Initiative. Bill earned a B.S. in Aerospace Engineering from the University of Michigan and worked in space systems engineering and project management at NASA and in Europe for a number of years. He later earned a Ph.D. in Neuroscience from U.C. Davis and held a faculty appointment in Radiology at UC San Francisco and research appointments at the Santa Lucia Institute in Rome. He also consulted on major projects for industry and academia.

*

Dave Nalley, The Apache Foundation - Vice President, Infrastructure

*

Anita Nikolich is Program Director for Cybersecurity in the Division of Advanced Cyberinfrastructure at the National Science Foundation (NSF). Prior to her work at the NSF she served as the Executive Director of Infrastructure at the University of Chicago. Past assignments include Director of Global Data Networking at Aon and Director of Security for Worldcom. She has explored how information technology and secure networking can best support the creation and sharing of scientific knowledge in virtual, mobile and physical contexts. She holds a Master of Science from The University of Pennsylvania and a Bachelor of Arts from the University of Chicago.

*

Amy Northcutt was appointed Chief Information Officer of the National Science Foundation in January 2012. In this capacity, she is responsible for NSF's information technology investments,

governance, policy, and planning. Prior to this appointment, Ms. Northcutt served as Deputy General Counsel of the Foundation from 2001 - 2012. Ms. Northcutt holds a J.D., magna cum laude, from Boston College Law School, an A.M.R.S. from the University of Chicago; and a B.A. from Smith College.

*

Susan Ramsey, University Corporation for Atmospheric Research - Security Engineer, CEH, CPT

*

Douglas Richardson is the Executive Director of the Association of American Geographers (AAG), a scholarly association of 11,000 members dedicated to the advancement of geographic research, scholarship, and education. Richardson has led a successful organizational renewal at the AAG during the past twelve years. He has expanded its membership greatly, developed strategic new research and educational initiatives, and extended the AAG's international reach and programs substantially. He has built a strong financial foundation for the AAG and for geography's future.

Prior to joining the AAG, Dr. Richardson founded and was the president of GeoResearch, Inc., a private research firm specializing in the environmental and geographical sciences. Richardson and GeoResearch invented, developed, and patented the world's first real-time interactive GPS/GIS technologies, which have transformed the ways in which geographic information is now collected, mapped, integrated, and used within geography, as well as in society at large. He sold the company and its core patents in 1998.

His current research interests include GIScience dimensions of health, and real interactive time-space time integration in geography and GIScience. He has served on numerous private, public, and NGO boards and committees, including currently the National Geospatial Advisory Committee, chairing its Geospatial Privacy Subcommittee.

*

Scott Sakai, San Diego Supercomputer Center at UCSC - Cyber Security Specialist

*

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, surgical suture manufacture, biopharmaceuticals, specialty chemicals, laundry transport, semiconductor equipment manufacture, and nuclear power plant infrastructure. He is managing partner of Jeneriah, Industrial Automation.

*

Anurag Shankar is a senior security analyst at Indiana University's Center for Applied Cybersecurity Research (CACR). His expertise includes regulatory compliance (HIPAA and FISMA) and cybersecurity risk management. He has helped numerous institutions tackle HIPAA compliance and been responsible for developing a NIST based risk management framework and using it to align IU's central research cyberinfrastructure with HIPAA. Prior to joining CACR, he spent nearly two decades at IU developing, delivering, and managing Unix support, massive data storage, and the national Teragrid project, and supporting the research mission of the IU School of Medicine. He played a key part in

building several of IU's large data storage environments, for supporting IU's Indiana Genomics Initiative and other life sciences efforts, and for building an information infrastructure 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).

*

Abe Singer is the Chief Security Officer for the Laser Interferometer Gravitational Wave Observatory, operated by the California Institute of Technology. Previously he was the CSO of the San Diego Supercomputer Center at U.C. San Diego, and has had past lives as a private sector consultant, programmer, and system administrator.

*

Adam Slagell is the Director of Cybersecurity and Chief Information Security Officer at the National Center for Supercomputing Applications (NCSA). In addition to providing security leadership for the NCSA and the NSF-funded XSEDE federation, he has been a cybersecurity researcher and PI for several years in the areas of security visualization, anonymization, intrusion detection, and more. Currently he is the liaison for the Bro Project at the Software Freedom Conservatory and co-PI for the NSF Bro Center, which brings its network security monitoring expertise and support to NSF cyberinfrastructure and projects.

*

Susan Sons serves as a Senior Systems Analyst at Indiana University's Center for Applied Cybersecurity Research, having come from a background in abuse management, software development, and pentesting. In her free time, Susan volunteers as director of the Internet Civil Engineering Institute, a nonprofit dedicated to supporting and securing the common software infrastructure we all depend on, and as a search-and-rescue and disaster relief worker.

*

Amy Starzynski Coddens serves as the Education, Outreach and Training Manager at Indiana University's Center for Applied Cybersecurity Research (CACR). She is a graduate of the IU School of Education (M.S. '06 & M.S. '09). Amy comes to the CACR and CTSC from a background in P-16 education and outreach. She has worked for the government, in industry and in academia, contributing to projects with the New England Research Institute, Harvard's PEAR Institute, the United States Department of Education's Office of Special Education Programs, and the IU Kelley School of Business.

*

Karen Stocks received her PhD in Biological Oceanography from Rutgers University in 2000. She is the Director of the Geological Data Center (GDC) at Scripps Institution of Oceanography, where she is responsible for managing 50+ years of digital and analog data from Scripps research vessels. She also serves as the Director of Information Services for the Science Support Office of the Integrated Ocean Discovery Program. Her other current projects focus on the documentation, discovery, access, integration, and curation of oceanographic data. Her past experience includes information systems for biodiversity and biogeography, metagenomics, and ocean observing systems.

*

George Strawn had a short industrial career (4 years with IBM), a long academic career (30 years at Iowa State) and a pretty long government career (24 years at NSF). At Iowa State he served terms as chair of the Computer Science department and director of the Computation Center. At NSF he invented the Internet (well, he was NSFnet program director and then division director of networking) and then served as CIO. He was most recently detailed to OSTP where he served as director of the NITRD NCO until his retirement in July. He has a PhD in mathematics from Iowa State and is a fellow of AAAS.

*

Amar Takhar has worked on both software and hardware testing for 18 years. He has designed several complete testing systems for Continuous Integration, operational and structured testing. Amar has a strong passion for design conformance and quality assurance. He has been both a longtime contributor to the NTP and Buildbot and RTEMS projects.

*

Liviu Vâlsan serves as an IT security architect for CERN, the European Organization for Nuclear Research (http://cern.ch). His interests include systems design for Computer Security Operations Centers at a large scale. Liviu holds a Bachelor degree in Computer Science from Politehnica University of Bucharest and a Masters degree in IT Project Management from the Bucharest Academy of Economic Studies. He started working at CERN in 2008 as a Software Engineer and System Administrator with the ATLAS experiment at the Large Hadron Collider (LHC). Liviu joined CERN openlab in May 2012 as a staff Computing Engineer, taking an active role in the research and development efforts inside the Platform Competence Centre (PCC) while also managing the integration of (predominantly prototype) hardware and software inside the openlab environment. Since 2013 he is part of the CERN IT Computing Facility group responsible for the management and operation of the Computer Centre and associated Computing Facilities. He has ever since been involved in the procurement of thousands of servers and dozens of petabytes of disk storage yearly for the Worldwide LHC Computing Grid Tier-0 centre at CERN as well as for the many services run by other groups in the CERN IT department.

*

Kent Wada is UCLA chief privacy officer and director, strategic IT policy for the University of California, Los Angeles (UCLA).

Designated as campus's first chief privacy officer in 2012, Kent addresses foundational privacy issues that have broad impact on the campus community and the University mission through his role on the executive committee of the UCLA Board on Privacy and Data Protection. He collaborates closely with campus counsel, the chief information security officer, and many others, including the offices that have compliance authority for protection of personal information (chief compliance officer of UCLA Health, registrar, IRB, ...), to have UCLA be a good steward of this data.
In his role as director, strategic IT policy for the campus, Kent works broadly with the campus, UC system, and subject matter experts to help shape the institutional agenda for technology policy issues of strategic concern – whether privacy, copyright and illegal file sharing, IT accessibility, information security, or beyond. These issues become part of the campus IT planning and governance process though Kent's role as a member of the management team of the vice provost, Information

Technology and chief academic technology officer.

*

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 incidents, affecting multiple organizations and mission critical services. This implies focusing on malware, like rootkits, forensics, threat intelligence, and building international collaborations to prepare for and manage crisis. 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 Indiana University's Center for Applied Cybersecurity Research (CACR) and PI for the Center for Trustworthy Scientific Cyberinfrastructure, a project dedicated to tackling the cybersecurity challenge for NSF science. His expertise lies in applied research and practice of cybersecurity for distributed systems. Other roles include serving as CSO of the Software Assurance Market Place, a DHS-funded facility to foster software assurance and software assurance research, PI on a Department of Energy funded grant focused on identity management for extreme-scale scientific collaboration, and serving as a advisor for research on the InCommon Steering Committee. Previously he has worked with a range of high-visibility projects to provide cybersecurity to the broader scientific and engineering community, including TeraGrid, Open Science Grid, Ocean Observatory Infrastructure, and GENI. His work in software and standards includes authoring two IETF RFCS and the contributing to the creation of the well-known CILogon and MyProxy projects.

*

Dr. Carol Wilkinson is a visitor to NSF from the California Institute of Technology, providing support to the Large Facilities Office (LFO) on issues regarding the management of large scientific facilities. Her major roles while at NSF include being the LFO liaison to various facilities under construction, assisting with revisions of the Large Facilities Manual, and acting as the LFO liaison for Cyber Infrastructure. Her background includes research in experimental particle physics and experience in the operation and construction of large scientific facilities. She has formal training in facility and project management from the Project Management Institute (PMI) and other institutions. She earned certification in project management from the Stanford Advanced Project Management Institute.

Dr. Wilkinson gained familiarity with NSF construction projects funded through Major Research Equipment and Facility Construction (MREFC) accounts by serving for ten years as the project manager for the Advanced LIGO (Laser Interferometer Gravitational-Wave Observatory) development and construction. She also served on NSF construction project review panels for DUSEL, ALMA, OOI, NEON, and LSST. Previously, Dr. Wilkinson served as group leader and project manager for the construction and operation of two DOE funded accelerator facilities (DARHT) at Los Alamos National Laboratory before becoming project manager for the nuclear weapons testing program at DARHT before joining LIGO in 2003. She joined NSF on an Intergovernmental Personnel Act (IPA) assignment in November 2013.

*

Alexander Withers entered the field of cyber security 15 years ago as an intern at Idaho National Laboratory. He has since obtained a masters in computer science from Stony Brook University and

has worked in both high performance computing for the physics community and cyber security at Brookhaven National Laboratory. He current works for the Cyber Security Directorate at the NCSA where he focuses on cyber security research and policy.

Appendix C
Call for Participation

Call for Participation

2015 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure

August 17 - 19 ✶ Westin Arlington Gateway ✶ Arlington, VA

http://trustedci.org/2015summit/

Theme: *Understanding the Information Assets that Enable Science*

It is our great pleasure to announce that the 2015 Summit will take place Monday, August 17th through Wednesday, August 19th, at the Westin Arlington Gateway near the National Science Foundation Headquarters in Arlington, VA. On August 17th, the Summit will offer a full day of information security training tailored for the NSF community. The second and third days will follow a workshop format designed to increase the NSF and research community's understanding of the information assets that enable science: what our information assets are, what risks they face, and how to protect them.

About the Summit

Since 2004, the annual NSF Cybersecurity Summit has served as a valuable part of the process of securing the NSF scientific cyberinfrastructure by providing the community a forum for education, sharing experiences, building relationships, and establishing best practices.

The NSF cyberinfrastructure ecosystem presents an aggregate of complex cybersecurity needs (e.g., scientific data and instruments, unique computational and storage resources, complex collaborations) as compared to other organizations and sectors. This community has a unique opportunity to develop information security practices tailored to these needs, as well as break new ground on efficient, effective ways to protect information assets while supporting science. The Summit will bring together leaders in NSF cyberinfrastructure and cybersecurity to continue the processes initiated in 2013 and 2014: Building a trusting, collaborative community, and seriously addressing that community's core cybersecurity challenges.

The Summit seeks proposals for presentations, breakout and training sessions. It offers opportunities for student scholarships.

Proposing Content for the Summit

There are many ways to contribute to the Cybersecurity Summit. We are open to proposals for full- or half-day training sessions, for plenary presentations, and for breakout sessions. More specific information on each of those is available below. Submissions should be sent to CFP@trustedci.org by July 12th. Responses should go out by July 24th to ensure adequate planning time for presenters.

Proposing a Plenary Presentation

Please submit brief white papers focused on NSF Large Facilities' unmet cybersecurity challenges, lessons learned, and/or significant successes for presentation during the Summit Plenary Session (Aug 18-19). White papers (and presentations) may be in the form of position papers and/or narratives and may be one to five pages in length.

All submitted white papers will be included in the 2015 summit report. The Program Committee will select the most relevant, reasoned, and broadly interesting for presentation. A limited amount of funding is available to assist with travel for accepted submissions.

Submission deadline: July 12

Submit to: CFP@trustedci.org

Word limit: 400 to 2000 words (~1-5 single spaced pages)

Notification of acceptance: July 24

Proposing a Training Session

Training may be targeted at technical and/or management audiences, and be half-day or full-day in length. Areas of interest include, but are not limited to: cybersecurity planning and programs, risk assessment and management, regulatory compliance, identity and access management, data management and provenance, networks security and monitoring, secure coding and software assurance, physical security in the context of information security, and information security of scientific and emerging technologies. The Program Committee will select the most community-relevant and broadly interesting training sessions for presentation during the first day of the summit (Aug 17).

We generally prefer trainings with some hands-on or interactive component over those that can be equally well presented in a non-interactive format (e.g. online videos), whether that component is a series of review Q&As, the opportunity to work directly with a piece of software or other tool, or a planning/management activity.

Submission deadline: July 12

Submit to: CFP@trustedci.org

Word Limit: 600 words

Notification of Acceptance: July 24

Proposing Breakout Sessions and Other Activities

In past years, the Summit has experimented with other formats for networking and information exchange, such as table-top topics at lunch and breakout sessions. Proposals for such an activity should be 1-2 pages in length and include the time and space that would need to be allocated, who would run the activity, the activity's intended audience, and a description of the activity itself and its expected benefits.

Submission deadline: July 12

Submit to: CFP@trustedci.org

Word limit: 400 to 800 words (~1-2 single spaced pages)

Notification of acceptance: July 24

Information for Students

Each year, the summit organizers invite several students to attend the summit. Reimbursement of travel expenses may be available. See Call for Student Applications for more information.

Notes for First-Time Presenters

The Summit organizers want to encourage those who have not presented at previous Summits to share their experiences, expertise, and insights with the NSF cybersecurity community. You don't need to be perfectly polished, you just need to have something to share about your project or facility's experience with information security. Feedback from last year's Summit showed that there was a great deal of interest in "lessons learned" type presentations from projects who've faced cybersecurity challenges, and had to rethink some things afterwards. We've put together a page of tips and ideas for new presenters, including proposal and presentation tips as well as suggested topics. More direct coaching is available upon request.

Please contact CFP@trustedci.org with any questions, or to request help preparing a proposal or getting it ready to present at the Summit.

Appendix D
Training Descriptions

Training Sessions
August 17 2015 NSF Cybersecurity Summit

Monday, August 17 will feature a full day of training, available to all registrants. All but the Bro Platform Training Workshop and Developing Cybersecurity Programs for NSF Projects are half-day offerings. Seating may fill for some or all sessions, and pre-event registration for individual sessions is required to reserve a seat. Please register by August 12 to guarantee seating, and help us make final preparations. Direct inquiries to Amy Starzynski Coddens (astarzyn@indiana.edu).

Concurrent Morning Sessions

Bro Platform Training Workshop (Full Day)

Instructors: Justin Azoff (NCSA), Adam Slagell (NCSA), Johanna Amann (ICSI)

Bro is a powerful network analysis framework used for security monitoring and network analysis. The user community includes major universities, research labs, supercomputing centers, and government and corporate organizations. In order to gain the most utility out of Bro we encourage users to attend training workshops and participate in the greater online community. The NSF Cybersecurity Summit presents the ideal opportunity to fulfill our responsibility of supporting NSF-funded sites.

The Bro development team is prepared to deliver a full day workshop focusing on such topics as Bro administration, examining logs, learning out-of-the-box and custom Bro scripts, using Bro Control, and other new features in Bro's v2.4 release. The morning session will focus on explaining what is Bro, how it is used, and out-of-the-box features. The afternoon session will focus on topics for more experienced users.

Developing Cybersecurity Programs for NSF Projects (Full Day)

Instructors: Bob Cowles, Craig Jackson, Jim Marsteller, Susan Sons (CTSC)

Team members of the Center for Trustworthy Scientific Cyberinfrastructure (CTSC) will present two interactive half day sessions on developing cybersecurity programs for NSF science and engineering projects. Attendees may register for one or both sessions.

Morning Session. This instructional morning session will be based on a cybersecurity planning guide (see, trustedci.org/guide) developed with input from the Daniel K. Inouye Solar Telescope (DKIST) project, and in use at a

number of NSF facilities and projects. The Guide was developed to address the information security requirements outlined in NSF cooperative agreements, and provide solid guidance, tools, and resources. 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 a good deal of overlap, we will be updating our presentation, and supporting opportunities to explore areas in greater depth based on participants' needs. Some of the topics that will be covered include:

- Building or Improving and Information Security Program
- Unique and Critical Science Requirements, Constraints, and Security Controls
- Information Security Policies and Procedures
- The Role of Project Leadership and Risk Acceptance
- Establishing a Risk Management Approach to Information Security
- Defining, Identifying, and Classifying Information Assets
- The Role of Risk Assessments within the Program Lifecycle
- Baseline Controls and Best Practices
- Topical Information Security Considerations: Third-Party Relationships, Asset Management, Access Control, Physical Security, Monitoring, Logging, and Retention
- Program Assessment and Evaluation

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

Afternoon Session. We encourage registrants for this afternoon session to come prepared to share their experiences, ask questions, and learn from one another. The afternoon session will entail facilitated discussion and deep dives into two topics areas:

1) **Cyberscurity Program Governance, Risk Acceptance, and Intra-organization Communication**. In most organizations, the people writing code, maintaining the network, and administering systems have the most information about the organization's information assets and risks thereto. Most decisions about resourcing and risk acceptance, however, are made much higher up the chain, and the greatest concentration of information security expertise likely lies somewhere in between. Meanwhile, technologists and managers often have very different ways of thinking and communicating about information security issues. In this module, we'll talk about common failure modes in organizational management and communication around information security that can cause poor decisions in organizational risk management to be made on the back of bad information.

2) **Securing Novel Technologies**. Science often relies on specialized systems, including one-of-a-kind instruments and sensors, ICS/SCADA components, and custom software. Securing these systems requires more than applying industry best practices – by definition, mature best practices don't yet exist – it calls for technical analysis and communities of practice. In this module, we'll talk about helpful resources, and ways of tackling the security of these challenging systems.

Vulnerabilities, Threats, and Secure Coding Practices

Instructors: Barton P. Miller & Elisa Heymann

Security is crucial to the software that we develop and use. With the incredible growth of cyberinfrastructure services, security is becoming even more critical.

This tutorial is relevant to anyone wanting to learn about minimizing security flaws in the software they develop or manage. We share our experiences gained from performing vulnerability assessments of critical middleware. You will learn skills critical for software developers and analysts concerned with security.

This tutorial starts by presenting basic concepts related to threats, weaknesses and vulnerabilities. We will also show you how to think like an attacker. The rest of the tutorial presents coding practices that lead to vulnerabilities, with examples of how they commonly arise, techniques to prevent them, and exercises to reinforce your skills in avoiding them. Examples come from a wide variety of languages, including Java, C, C++, C# Perl, Python, and Ruby, and come from real code belonging to Web, Cloud and Grid systems we have assessed. This tutorial is an outgrowth of our experiences in performing vulnerability assessment of critical middleware and services including well-known systems such as Google Chrome, Wireshark, and HTCondor.

Industrial Control Systems, Networking, and Cybersecurity

Instructor: Phil Salkie

This presentation is a combination of three shorter programs originally presented at Penguicon 2014 and 2015: "Introduction to Programmable Controls," "Notes from the DHS ICS Cybersecurity 301 Class," and "Designing Secure Industrial Controls System Networks."

The training starts with an introduction to the basic hardware and software of modern industrial, scientific, and technical settings worldwide.

The next section is an overview of the monthly course offered by the Department of Homeland Security on securing ICS systems, its schedule, how to

apply for admission to the class, how to prepare in advance of attending, and what to expect from the week-long event.

The "Designing Secure ICS Networks" component is an effort to provide a foundation for assessing and improving legacy controls system networks as well as architecting new networks to maximize the security of ICS/SCADA systems. Participants will obtain a useable set of results, which flow from the lessons learned in the DHS course – sort of a "day six" of the five-day DHS curriculum.

Concurrent Afternoon Sessions

Bro Platform Training Workshop (continued)

See full description above.

Developing Cybersecurity Programs for NSF Projects (continued)

See full description above.

Aligning your Research Cyberinfrastructure with HIPAA and FISMA

Instructor: Anurag Shankar (Indiana University)

With biomedical research emerging as a formidable computing challenge needing support, providers of large scale research cyberinfrastructure such as high performance computing (HPC) shops are increasingly facing a new challenge, namely regulatory compliance. Also, new grants and contracts are beginning to require compliance with federal cybersecurity standards for protecting research data, whether or not biomedical. This half-day training session will familiarize participants with relevant regulations, how they apply, the challenges they present, and offer a standards-based risk management approach to tackling them.

Topics covered will include:

- *HIPAA and FISMA Demystified*. History and introduction to the regulations, what they mean for NSF facilities, what they do not.
- *The NIST Risk Management Framework*. Managing information security risk (NIST 800-39), conducting risk assessments (NIST 800-30), security and privacy controls (NIST 800-53), and assessing the controls (NIST 800-53A).
- *Leveraging the Framework*. Scoping, planning, implementing risk assessments, risk mitigation, documentation, ongoing risk management, reviews, and training, implementation at IU as example.

Incident Response Training

Instructor: Randy Butler (NSCA)

Computer incident response is a required capability for any project or activity that is running internet connected services. This tutorial will provide basic information on setting up an incident response program so that the students can prepare their project team or organization for handling an incident investigation. The initial focus of the tutorial will be on identifying the processes, policies, information, and monitoring services that will be required to effectively respond to a security incident. This first section will additionally discuss investigation and analysis tools that might be useful for investigations. The second part of the tutorial will identify a series of questions that the incident response team can use to guide them through both the investigation and the mitigation process. The final section will highlight several actual security incidents. Each of these incidents will be discussed in detail starting with how the incident was discovered and then continue through the investigation and mitigation process. The participant should leave the session with an understanding of the basic steps needed to create an incident response program and what to do when an incident occurs.

Appendix E
Listing of Attendees and Organizations

Appendix G: Listing of Attendees and Organizations

Last Name	First Name	Organization Provided
Adams	Andrew	CTSC/Pittsburgh Supercomputing Center
Allan	Jamie	Ocean Drilling Program National Science Foundation
Allar	Jared	Pittsburgh Supercomputing Center
Amann	Johanna	International Computer Science Institute
Apon	Amy	National Science Foundation
Azoff	Justin	NCSA
Babcock Hughes	James	AURA Inc.
Baldwin	Dora	California State University, San Bernardino
Barnet	Steve	UW-Madison - IceCube
Barton	Tom	University of Chicago
Basney	Jim	NCSA
Baylis	Tony	Lawrence Livermore National Laboratory
Bevier	RuthAnne	California Institute of Technology
Bryson	Matt	Lawrence Berkeley National Lab University of California Berkeley TRUST REU California Lutheran University
Butler	Randy	NCSA
Coles	Mark	NSF
Collmann	Jeff	Georgetown University
Cooper	Leslee	CACR
Corn	Michael	Brandeis University
Cowles	Bob	Indiana University / CACR
Davoudi	Ana	University of Central Florida
Dopheide	Jeannette	National Center for Supercomputing Applications
Dunaway	Tim	U.S. Army Corps of Engineers ERDC DoD Supercomputing Resource Center
DuRousseau	Don	George Washington University
Dykstra	Dave	Fermilab
Fleming	Mike	NOAO/AURA
Fleury	Terry	University of Illinois / NCSA
Flidr	Jaroslav	The George Washington University
Gates	Philip	International Ocean Discovery Program Texas A&M University
Gillies	Kim	Thirty Meter Telescope
Goodwin	Dave	U.S. Dept of Energy (DOE)
Greenspan	Sol	NSF
Halstead	David	National Radio Astronomy Observatory
Harris	Charlise	The Pennsylvania State University, Class of 2014

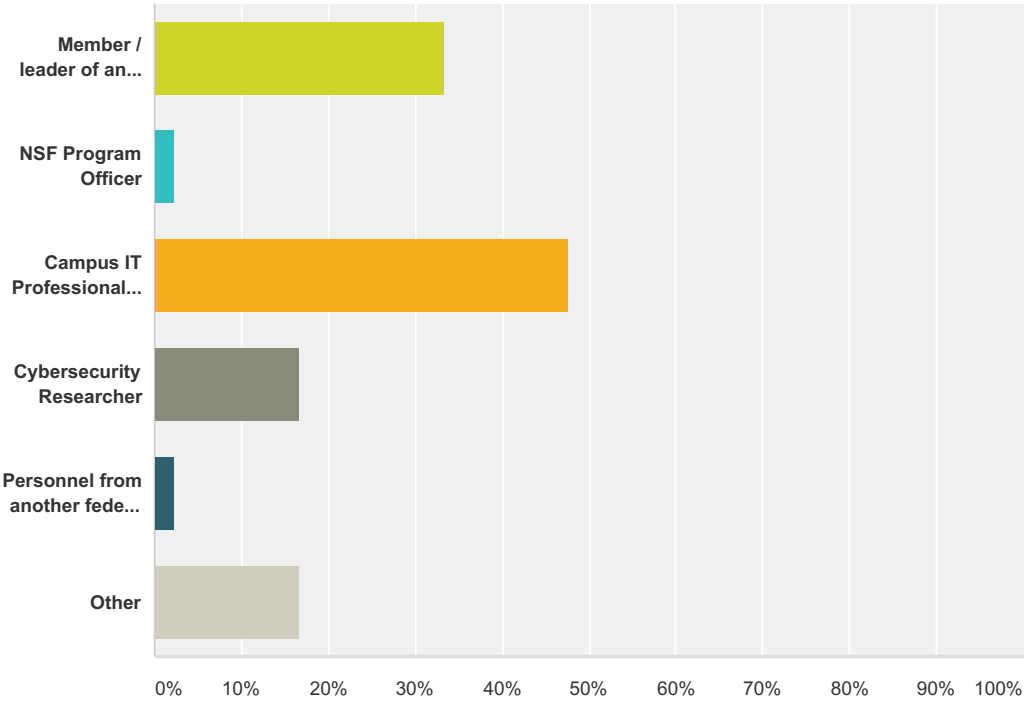
Hassler	Ardoth	Georgetown University
Hazlewood	Victor	University of Tennessee Joint Institute for Computational Sciences & XSEDE
Hernandez	Jary	West Virginia University Oak Ridge National Laboratory
Heymann	Elisa	University of Wisconsin-Madison
Housell	Jim	Rutgers Discovery Informatics Institute Rutgers, The State University of New Jersey
Houtman	Bob	National Science Foundation
Howard	Tim	National Science Foundation Division of Polar Programs
Jackson	Craig	CTSC / Indiana U.
Jacobs	Clifford	Clifford A. Jacobs Consulting, LLC
Jadoon	Aamir	Rutgers University
Jensen	Peter	National High Magnetic Field Laboratory
Kiser	Ryan	Indiana University Center for Applied Cybersecurity Research
Koranda	Scott	University of Wisconsin-Milwaukee
Krenz	Mark	IU Center for Applied Cybersecurity Research
Kurz	Ken	University of Oklahoma
Livny	Miron	University of Wisconsin - Madison
Markham	Brian	George Washington University - Division of IT
Marsteller	James A.	PSC/CMU
McElroy	Charles	Information Systems Case Western Reserve University
McGovern	Jean	NSF
Mendoza	Nathaniel	TACC/UT
Milford	Kim	REN-ISAC
Miller	Barton	University of Wisconsin
Miller	William	NSF CISE-ACI
Milton	Leslie C.	U.S. Army Engineer Research & Development Center
Minick	Tim	Gemini Observatory
Morrison	Chris	Gemini Observatory
Muñoz	José	NSF
Murphy	Pat	National Radio Astronomy Observatory
Nikolich	Anita	NSF
Pauschke	Joy	National Science Foundation
Petersen	Rodney	NIST
Pointer	Suzi	Indiana University CACR Center for Applied Cybersecurity Research
Quick	Rob	Indiana University
Ramsey	Susan	UCAR
Richardson	Douglas	Association of American Geographers
Richmond	Ryan L.	Association of Universities for Research in Astronomy (AURA)

Rieker	Tom	NSF
Sakai	Scott	San Diego Supercomputer Center at UCSD
Saunders	Yolanda	Bayfirst Solutions/DHS Science and Technology
Shankar	Anurag	Indiana University
Singer	Abe	LIGO California Institute of Technology
Slagell	Adam	NCSA/UIUC
Smith	Patrick D.	National Science Foundation Geosciences Directorate Division of Polar Programs
Sons	Susan	CACR, Indiana University
Spencer	Kristin	National Science Foundation BFA/DACS
Starzynski Coddens	Amy	Indiana University, CACR
Stengel	Brian	Technology Services (CSSD) University of Pittsburgh
Stocks	Karen	Scripps Institution of Oceanography
Strawn	George	NSF (retired)
Sun	Werner	CHESS/CLASSE, Cornell University
Takhar	Amar	RTEMS Project
Thompson	Kevin	NSF
Tuecke	Steve	Globus / UChicago / Argonne
Valsan	Liviu	CERN
Vieglais	Dave	University of Kansas
Walker	Ed	NSF
Walton	Amy	NSF
Wartel	Romain	CERN
Welch	Von	Indiana University CACR
Wilkinson	Carol	NSF Large Facilities Office
Williams	Jason	Maryland Advanced Research Computing Center Johns Hopkins University
Withers	Alexander	NCSA

Appendix F
Attendee Survey Summary Report

Q1 Which options best describe your job or position? Check all that apply.

Answered: 42 Skipped: 0



Answer Choices	Responses	
Member / leader of an NSF project	**33.33%**	14
NSF Program Officer	**2.38%**	1
Campus IT Professional / CIO	**47.62%**	20
Cybersecurity Researcher	**16.67%**	7
Personnel from another federal program (NSA, DOE/ESNet, etc.)	**2.38%**	1
Other	**16.67%**	7
Total Respondents: 42		

Q2 Where do you work primarily?

Answered: 40 Skipped: 2

Answer Choices	Responses	
State/Province:	**100.00%**	40
Country:	**97.50%**	39

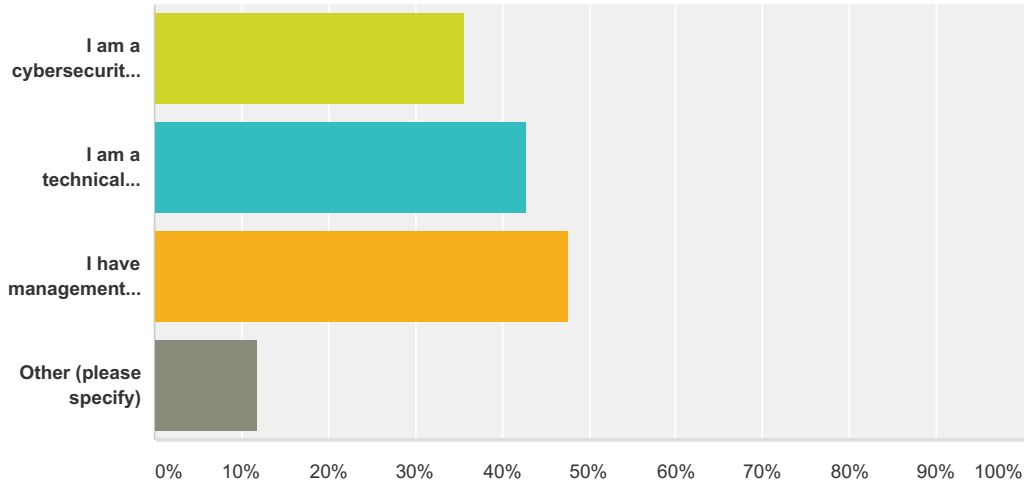
#	State/Province:	
1	Texas	
2	CA	
3	Indiana	
4	Washington, DC	
5	Pennsylvania	
6	MD	
7	California	
8	Texas	
9	IL	
10	Colorado	
11	Ontario	
12	Arizona	
13	Florida	
14	NY	
15	Coquimbo (La Serena)	
16	WI	
17	Washington	
18	VA	
19	Washington, DC	
20	Illinois	
21	PA	
22	California	
23	DC	
24	OK	
25	Arlington, VA	
26	CA	
27	CA	
28	Indiana	
29	La Serena	
30	Hawaii	
31	IL	
32	WI	

33	California	
34	tucson az	
35	Washington DC	
36	VA	
37	Knoxville, TN	
38	Florida	
39	VA	
40	Ohio	
#	**Country:**	
1	United States	
2	USA	
3	USA	
4	USA	
5	USA	
6	US	
7	USA	
8	USA	
9	USA	
10	USA	
11	Canada	
12	USA	
13	USA	
14	USA	
15	Chile	
16	USA	
17	DC	
18	US	
19	USA	
20	USA	
21	USA	
22	USA	
23	USA	
24	USA	
25	USA	
26	USA	
27	USA	
28	US	
29	Chile	
30	USA	
31	USA	
32	USA	

33	usa	
34	USA	
35	USA	
36	United States	
37	USA	
38	USA	
39	usa	

Q3 How would you characterize your job in relationship to cybersecurity? Please check all that apply.

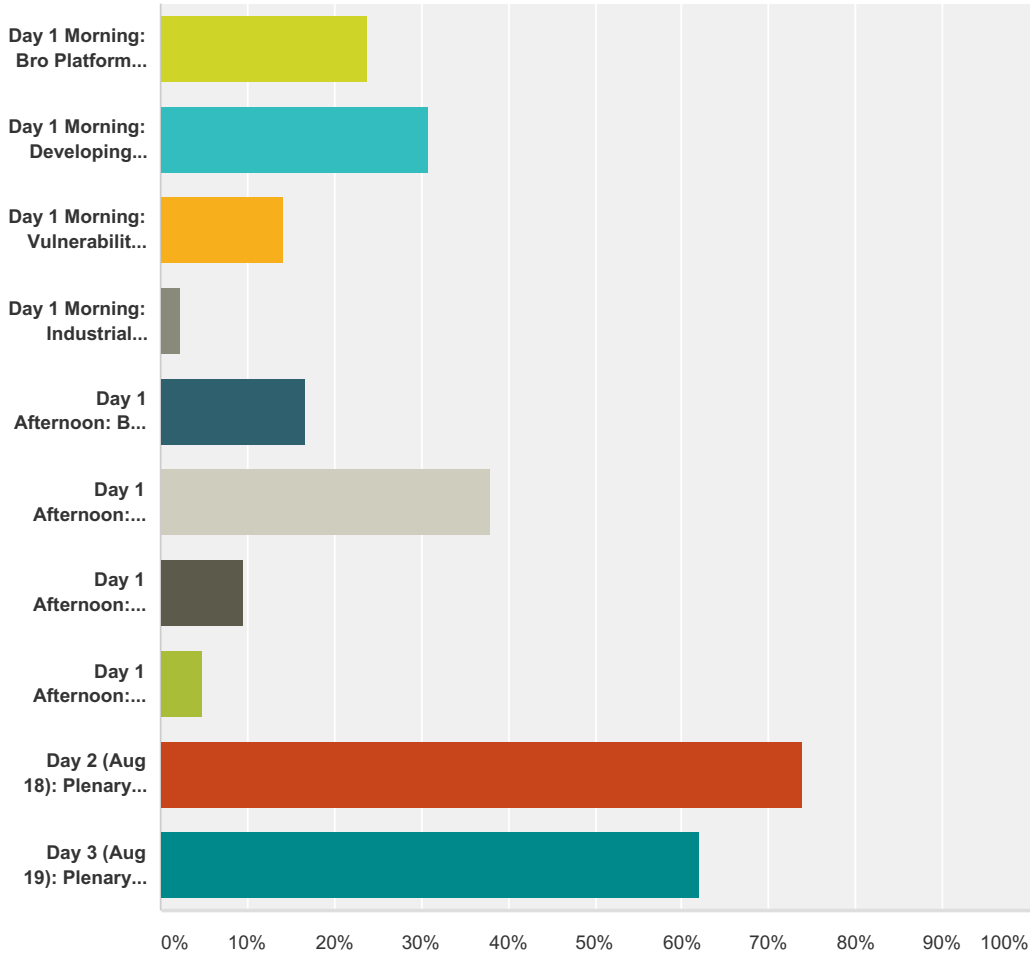
Answered: 42 Skipped: 0



Answer Choices	Responses	
I am a cybersecurity professional	**35.71%**	15
I am a technical professional who has knowledge of cybersecurity	**42.86%**	18
I have management responsibility for cybersecurity	**47.62%**	20
Other (please specify)	**11.90%**	5
Total Respondents: 42		

Q4 What sessions of the summit did you attend? Check all that apply.

Answered: 42 Skipped: 0

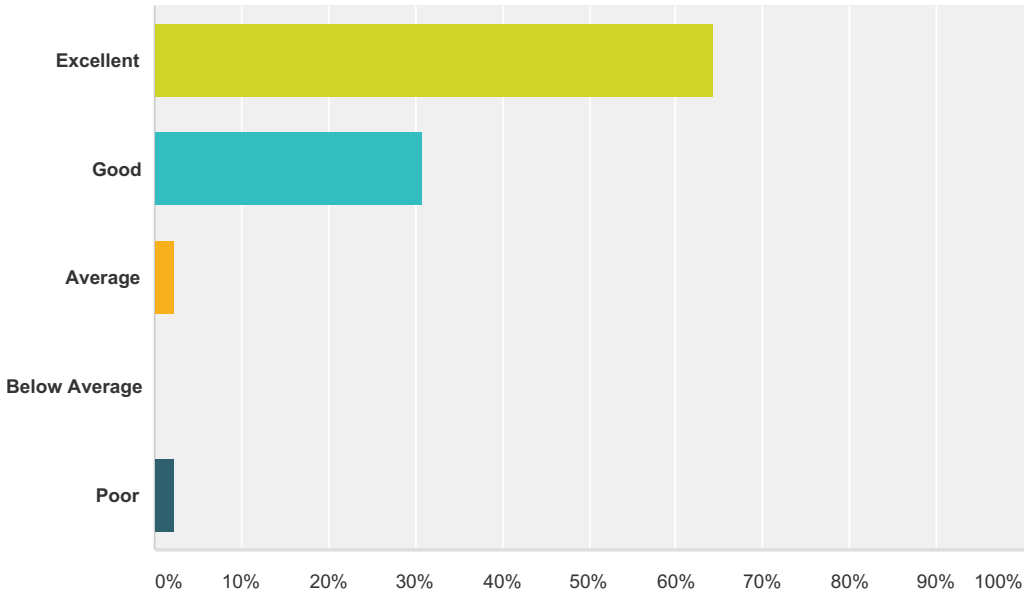


Answer Choices	Responses	
Day 1 Morning: Bro Platform Training Workshop	**23.81%**	10
Day 1 Morning: Developing Cybersecurity Programs for NSF Projects	**30.95%**	13
Day 1 Morning: Vulnerabilities, Threats, and Secure Coding Practices	**14.29%**	6
Day 1 Morning: Industrial Control Systems, Networking, and Cybersecurity	**2.38%**	1
Day 1 Afternoon: Bro Platform Training Workshop (continued)	**16.67%**	7
Day 1 Afternoon: Developing Cybersecurity Programs for NSF Projects (continued)	**38.10%**	16
Day 1 Afternoon: Incident Response Training	**9.52%**	4
Day 1 Afternoon: Aligning your Research Cyberinfrastructure with HIPAA and FISMA	**4.76%**	2
Day 2 (Aug 18): Plenary Session	**73.81%**	31
Day 3 (Aug 19): Plenary Session	**61.90%**	26

Total Respondents: 42	

Q5 How would you rate your overall experience with the 2015 summit?

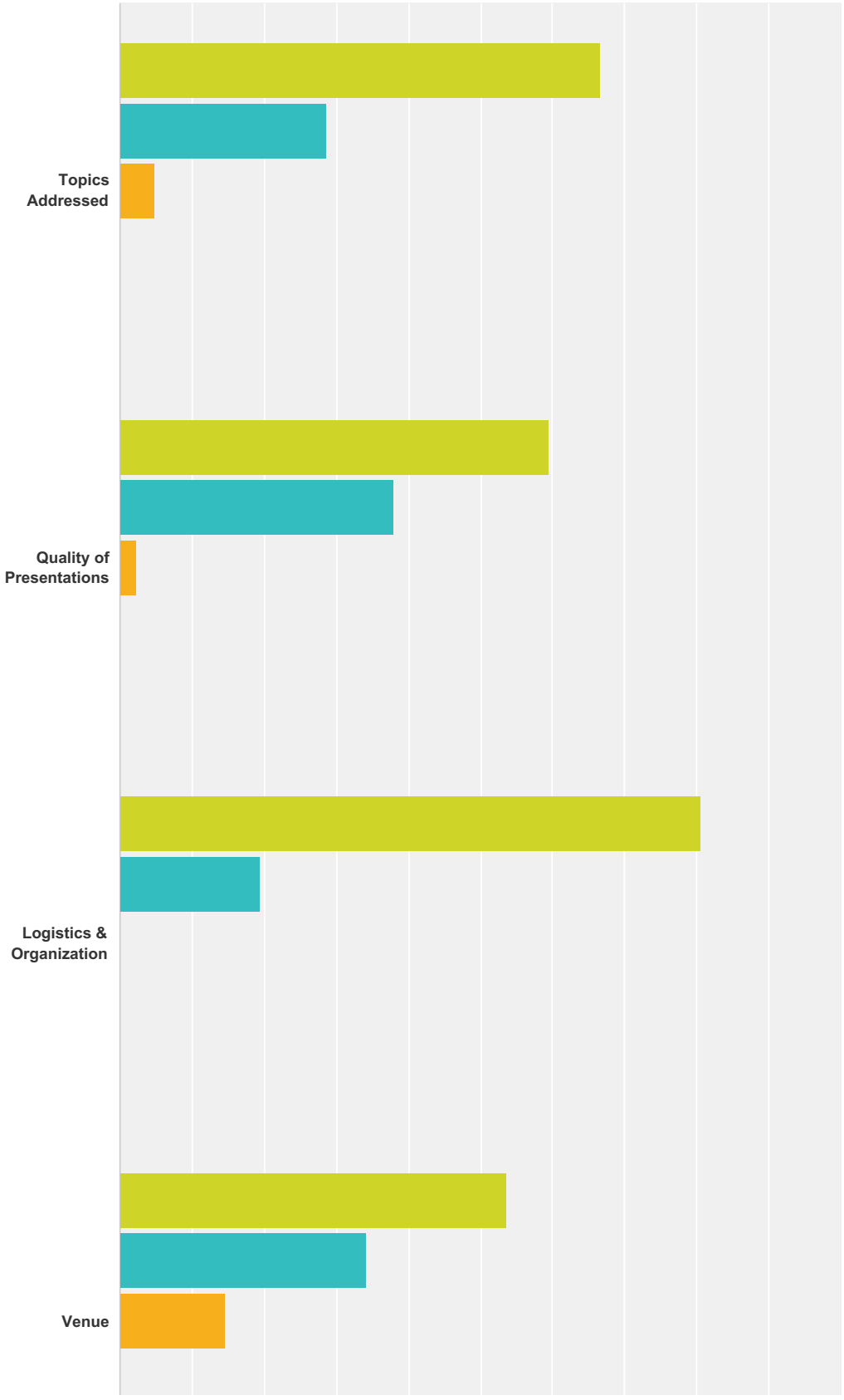
Answered: 42 Skipped: 0

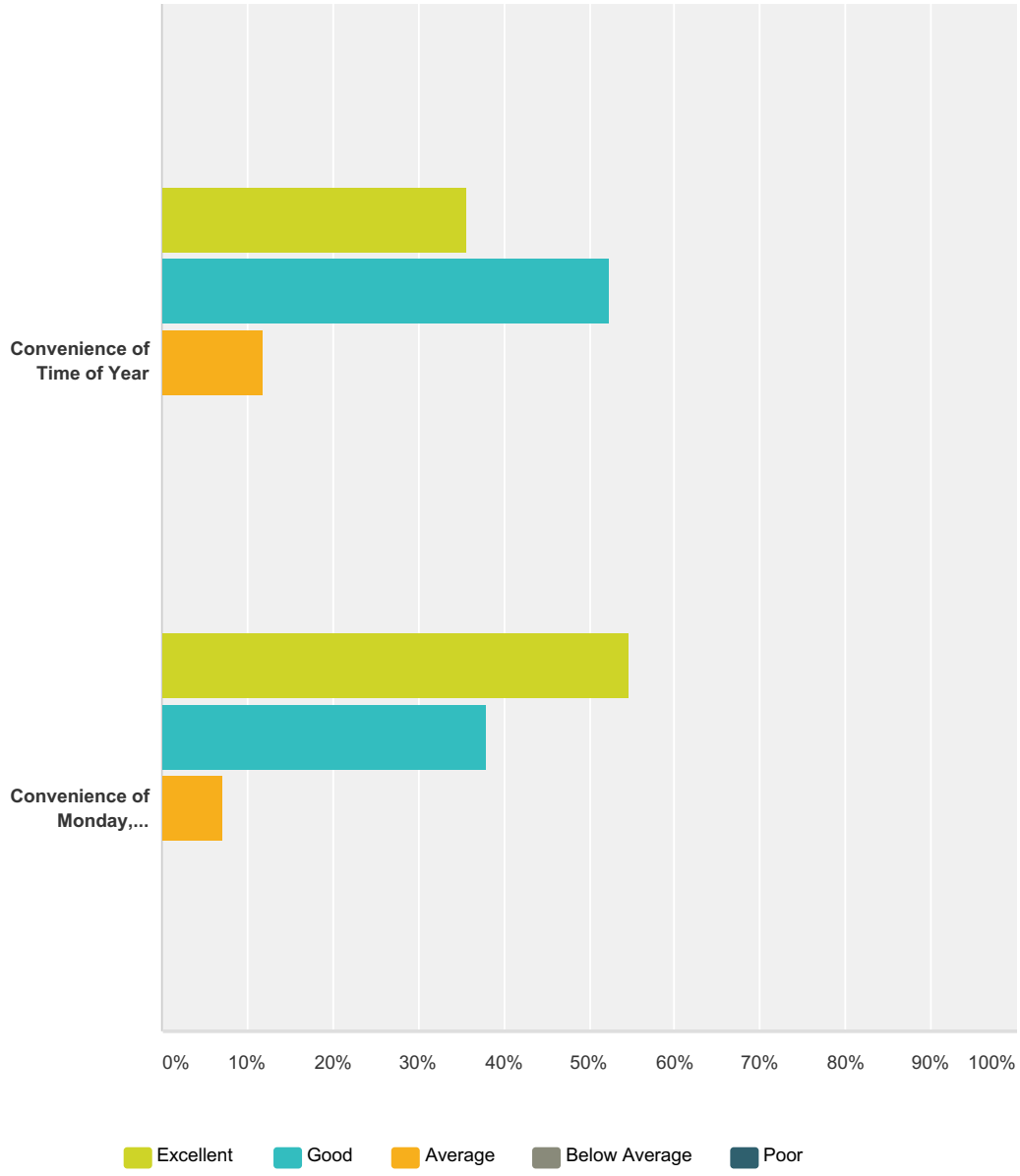


Answer Choices	Responses	
Excellent	**64.29%**	27
Good	**30.95%**	13
Average	**2.38%**	1
Below Average	**0.00%**	0
Poor	**2.38%**	1
Total		**42**

Q6 Please rate your experience with the 2015 summit in these areas:

Answered: 42 Skipped: 0

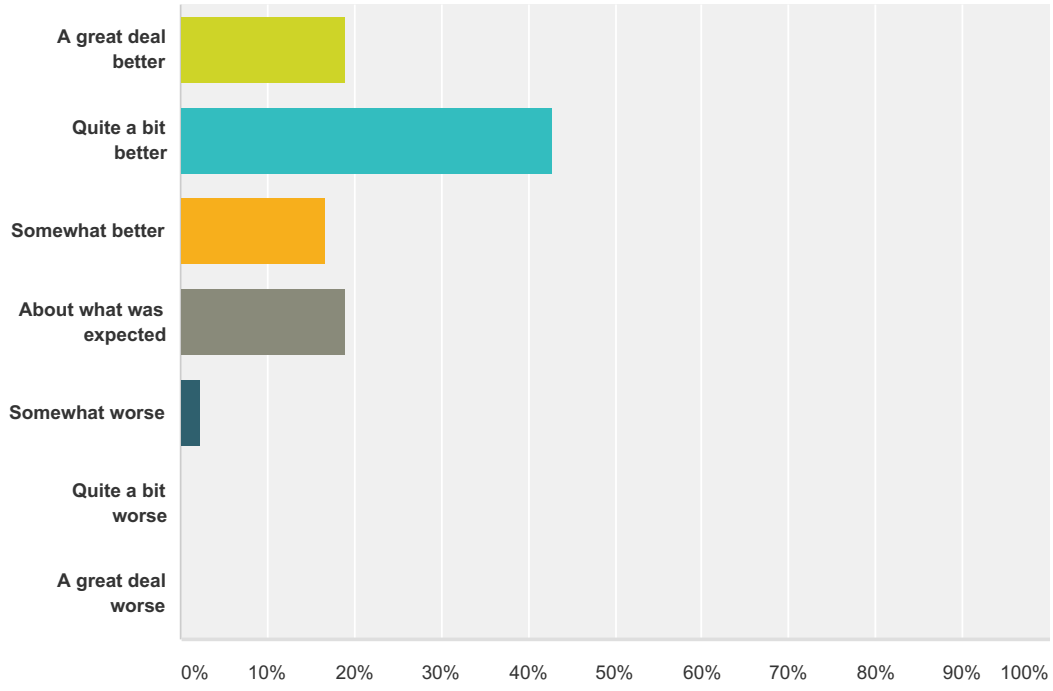




	Excellent	Good	Average	Below Average	Poor	Total Respondents
Topics Addressed	**66.67%** 28	**28.57%** 12	**4.76%** 2	**0.00%** 0	**0.00%** 0	42
Quality of Presentations	**59.52%** 25	**38.10%** 16	**2.38%** 1	**0.00%** 0	**0.00%** 0	42
Logistics & Organization	**80.49%** 33	**19.51%** 8	**0.00%** 0	**0.00%** 0	**0.00%** 0	41
Venue	**53.66%** 22	**34.15%** 14	**14.63%** 6	**0.00%** 0	**0.00%** 0	41
Convenience of Time of Year	**35.71%** 15	**52.38%** 22	**11.90%** 5	**0.00%** 0	**0.00%** 0	42
Convenience of Monday, Tuesday, Wednesday Dates	**54.76%** 23	**38.10%** 16	**7.14%** 3	**0.00%** 0	**0.00%** 0	42

Q7 Was this summit better than what you expected, worse than what you expected, or about what you expected?

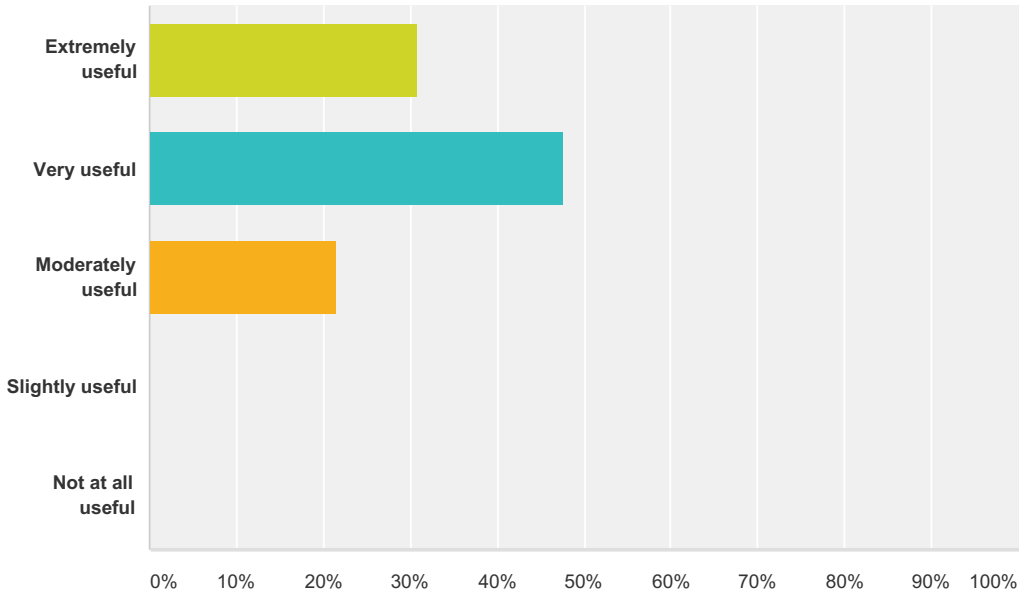
Answered: 42 Skipped: 0



Answer Choices	Responses	
A great deal better	**19.05%**	8
Quite a bit better	**42.86%**	18
Somewhat better	**16.67%**	7
About what was expected	**19.05%**	8
Somewhat worse	**2.38%**	1
Quite a bit worse	**0.00%**	0
A great deal worse	**0.00%**	0
Total		**42**

Q8 How useful to your work was the information discussed at the summit?

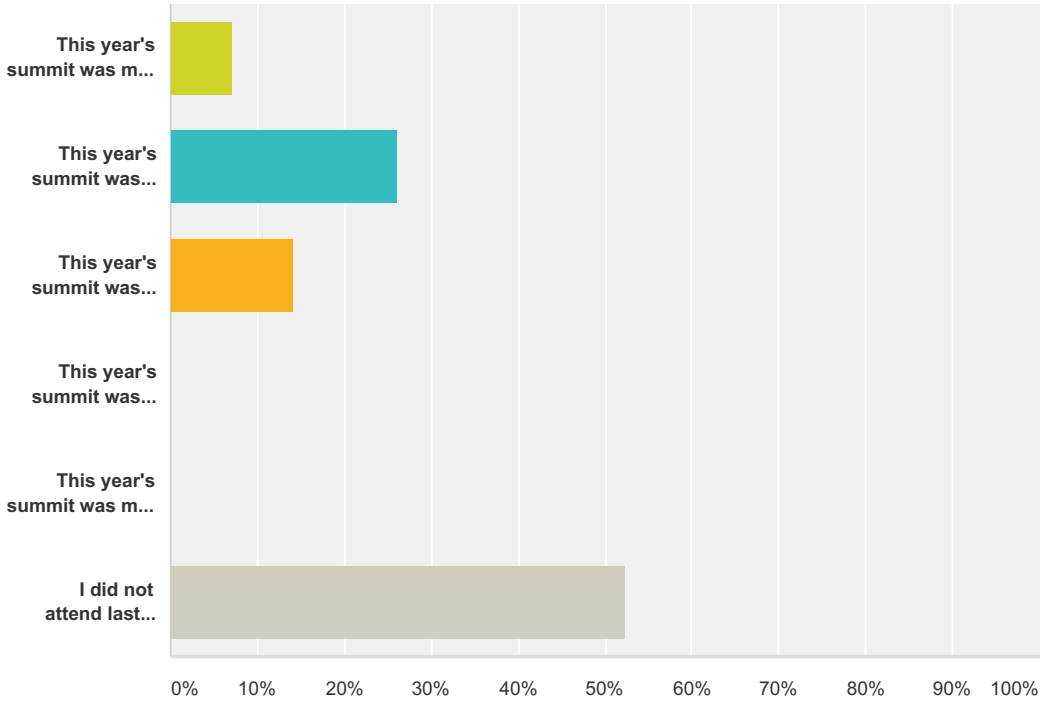
Answered: 42 Skipped: 0



Answer Choices	Responses	
Extremely useful	**30.95%**	13
Very useful	**47.62%**	20
Moderately useful	**21.43%**	9
Slightly useful	**0.00%**	0
Not at all useful	**0.00%**	0
Total		**42**

Q9 If you attended last year's summit, how does this year's compare?

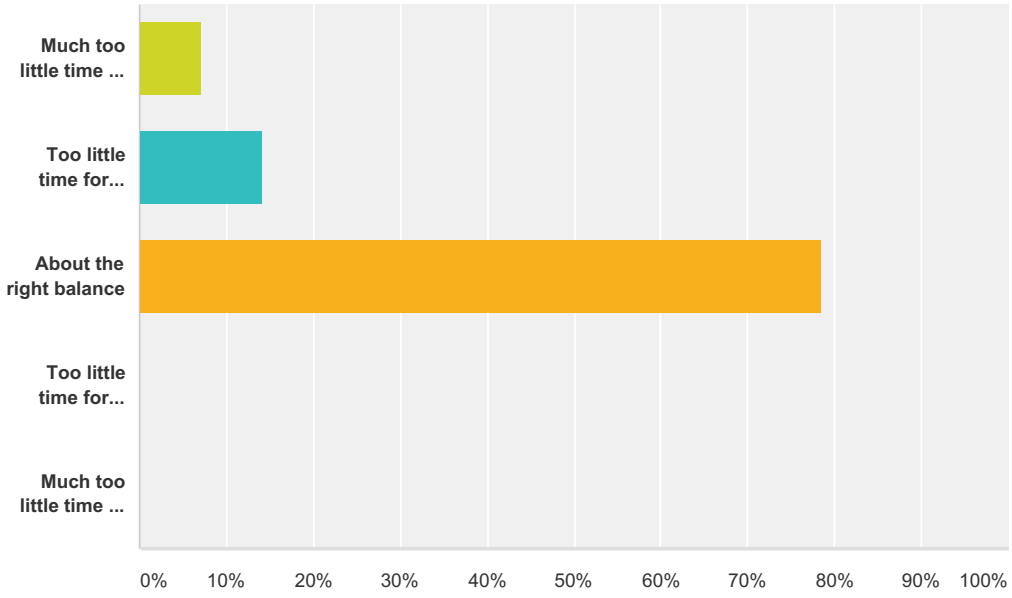
Answered: 42 Skipped: 0



Answer Choices	Responses	
This year's summit was much better than last year's.	**7.14%**	3
This year's summit was better than last year's.	**26.19%**	11
This year's summit was about the same as last year's.	**14.29%**	6
This year's summit was worse than last year's.	**0.00%**	0
This year's summit was much worse than last year's.	**0.00%**	0
I did not attend last year's summit.	**52.38%**	22
Total		**42**

Q10 How would you describe the balance between structured presentations and informal networking opportunities?

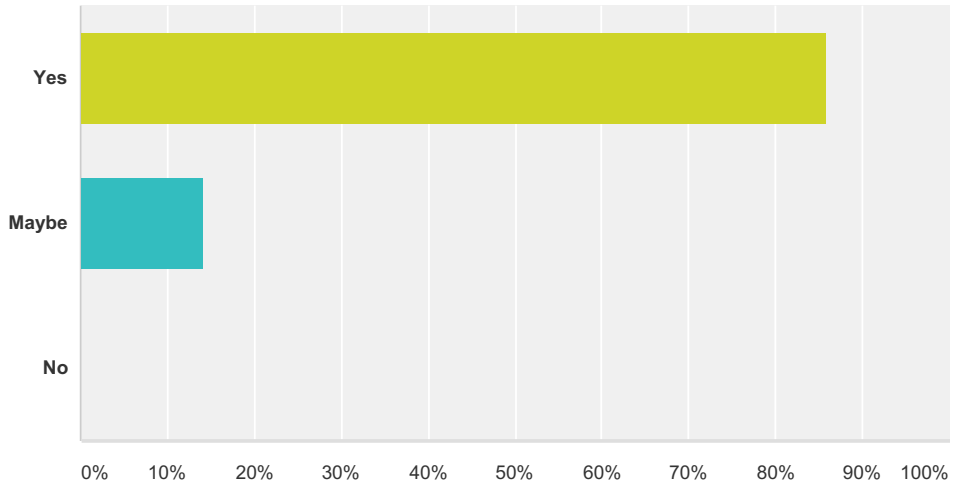
Answered: 42 Skipped: 0



Answer Choices	Responses	
Much too little time for informal networking	**7.14%**	3
Too little time for informal networking	**14.29%**	6
About the right balance	**78.57%**	33
Too little time for structured presentations	**0.00%**	0
Much too little time for structured presentations	**0.00%**	0
Total		**42**

Q11 Would you like to attend future summits?

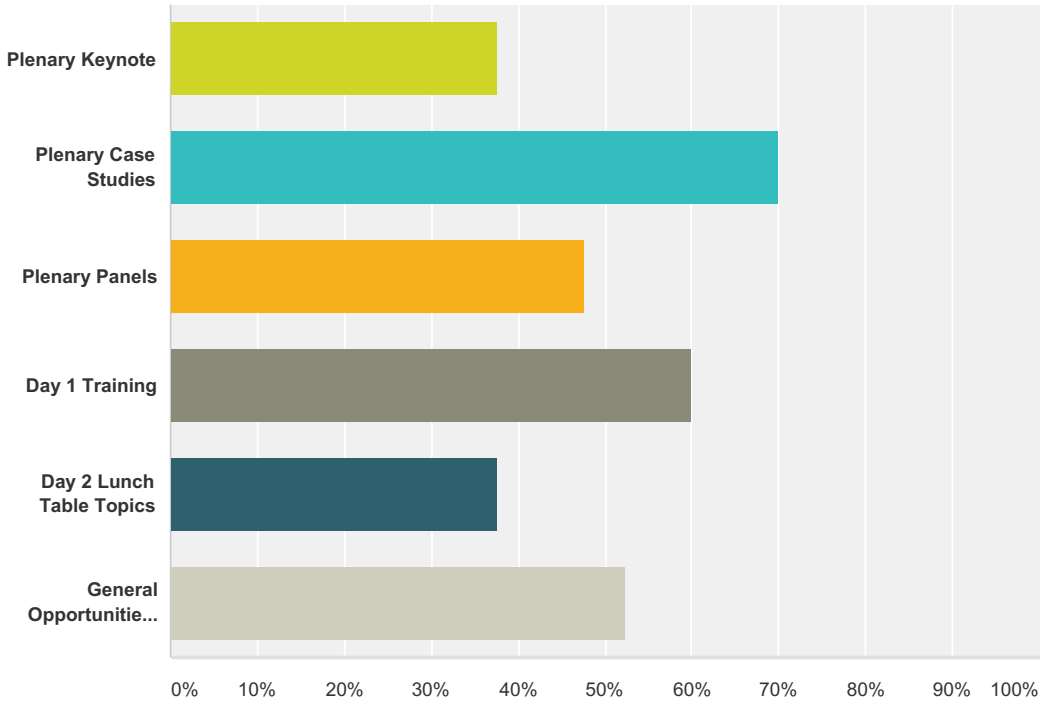
Answered: 42 Skipped: 0



Answer Choices	Responses	
Yes	**85.71%**	36
Maybe	**14.29%**	6
No	**0.00%**	0
Total		**42**

Q12 What presentation format(s) did you find most valuable? (You may select more than one.)

Answered: 40 Skipped: 2

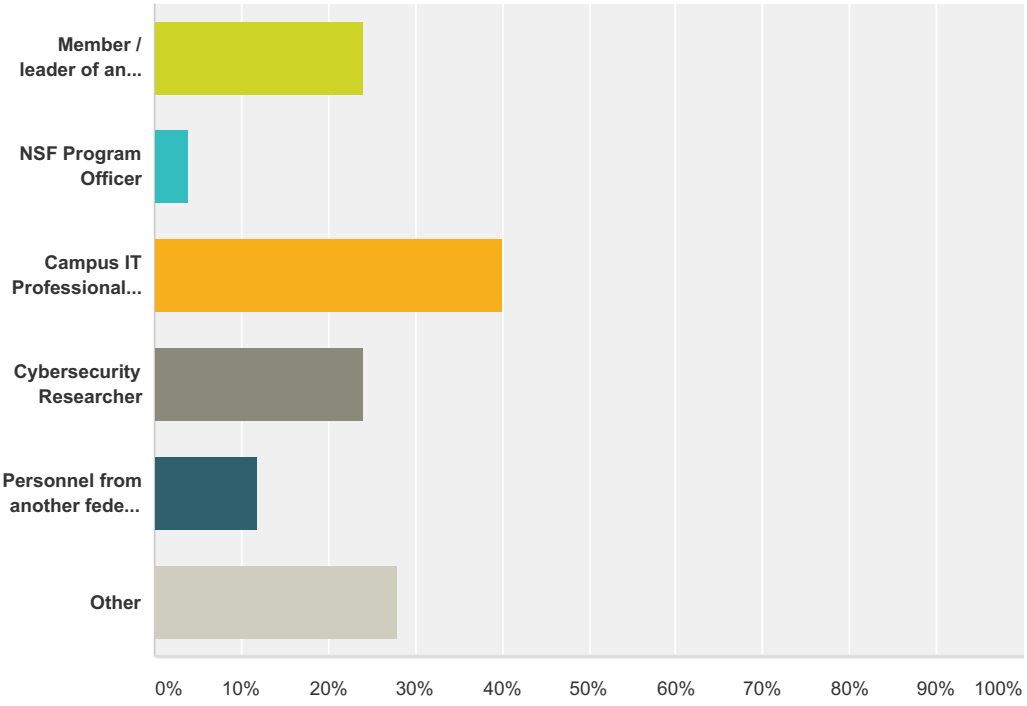


Answer Choices	Responses	
Plenary Keynote	**37.50%**	15
Plenary Case Studies	**70.00%**	28
Plenary Panels	**47.50%**	19
Day 1 Training	**60.00%**	24
Day 2 Lunch Table Topics	**37.50%**	15
General Opportunities to Network	**52.50%**	21
Total Respondents: 40		

Appendix G
Training Evaluation Survey Summary Report

Q1 Which options best describe your job or position? Check all that apply.

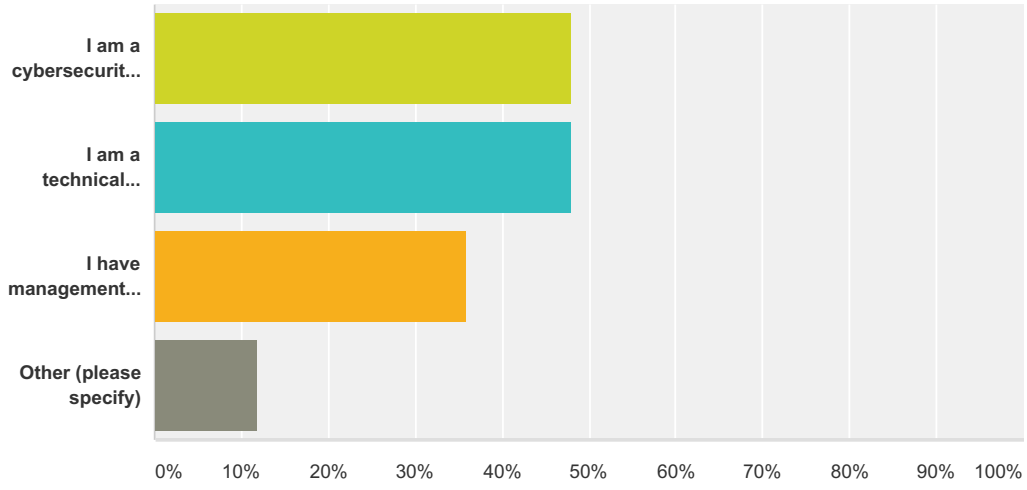
Answered: 25 Skipped: 0



Answer Choices	Responses	
Member / leader of an NSF project	**24.00%**	6
NSF Program Officer	**4.00%**	1
Campus IT Professional / CIO	**40.00%**	10
Cybersecurity Researcher	**24.00%**	6
Personnel from another federal program (NSA, DOE/ESNet, etc.)	**12.00%**	3
Other	**28.00%**	7
Total Respondents: 25		

Q2 How would you characterize your job in relationship to cybersecurity? Please check all that apply.

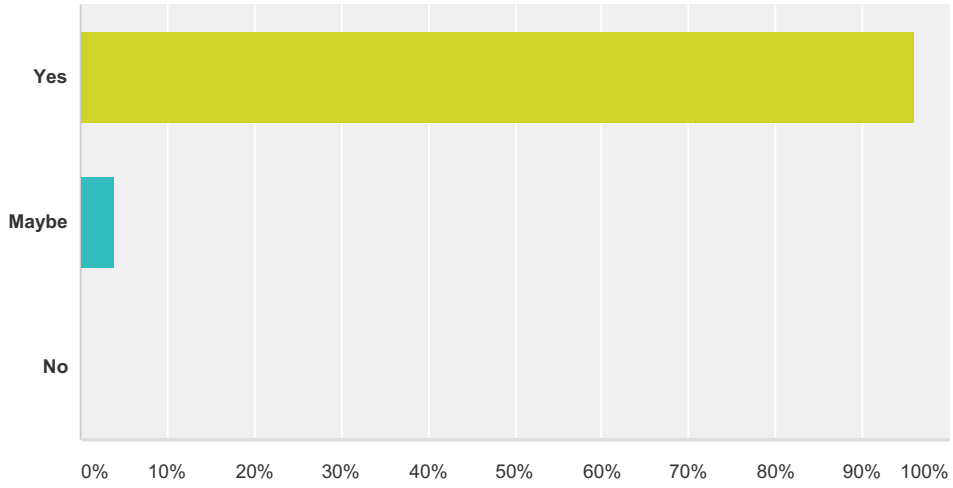
Answered: 25 Skipped: 0



Answer Choices	Responses	
I am a cybersecurity professional	**48.00%**	12
I am a technical professional who has knowledge of cybersecurity	**48.00%**	12
I have management responsibility for cybersecurity	**36.00%**	9
Other (please specify)	**12.00%**	3
Total Respondents: 25		

Q3 Based on your overall experience with the August 17 training sessions, would you participate in training offered at future summits?

Answered: 25 Skipped: 0



Answer Choices	Responses	
Yes	**96.00%**	24
Maybe	**4.00%**	1
No	**0.00%**	0
Total		**25**

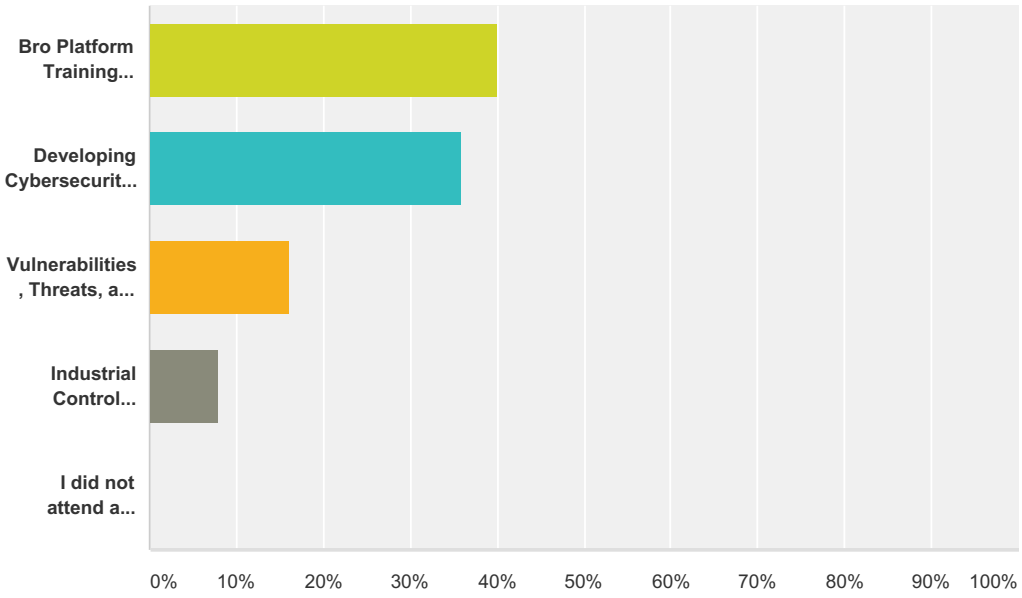
Q4 What training topics would you like to see covered at future summits?

Answered: 10 Skipped: 5

#	Responses	
1	- Given the emphasis on a risk-based approach to security, how about doing an actual risk assessment using CTSC guides? - Interfacing with the executive (, user, layman). It's easy to get caught up in technical lingo and leave non-security professionals confused and frustrated. How do you effectively present policy, procedure, and technical concepts to non-technical people?	
2	Open source solutions to Cybersecurity problems.	
3	In-depth howto type session for deploying federated identity?	
4	More in-depth training on Certified Ethical Hacking; perhaps a training session on Cyber Forensics	
5	Further vulnerability assessment, more advanced.	
6	Preparing for and designing a federated identity management infrastructure.	
7	Case studies are always good.	
8	social engineering; forensics;	
9	Something related to identity management would be good (technology review, procedures, concerns, best practices etc).	
10	Hands on ICS. Today was a good chance to see some of the actual devices in use. Perhaps a bit more on the way they work and interconnect.	

Q5 Which morning session did you attend?

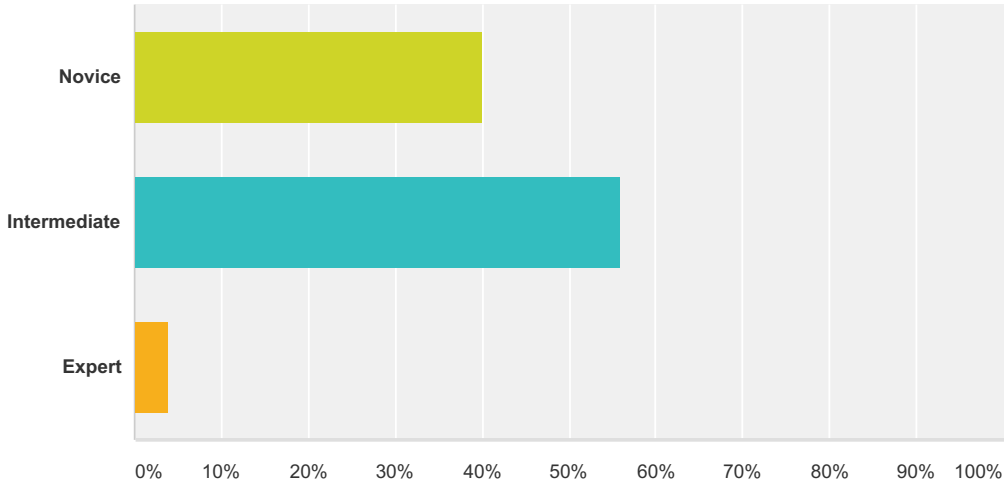
Answered: 25 Skipped: 0



Answer Choices	Responses	
Bro Platform Training Workshop (Justin Azoff, Adam Slagell & Johanna Amann)	**40.00%**	10
Developing Cybersecurity Programs for NSF Projects (CTSC Team)	**36.00%**	9
Vulnerabilities, Threats, and Secure Coding Practices (Barton P. Miller & Elisa Heymann)	**16.00%**	4
Industrial Control Systems, Networking, and Cybersecurity (Phil Salkie)	**8.00%**	2
I did not attend a morning session	**0.00%**	0
Total		**25**

Q6 How would you rate your level of pre-training familiarity with the topics covered by this morning training session?

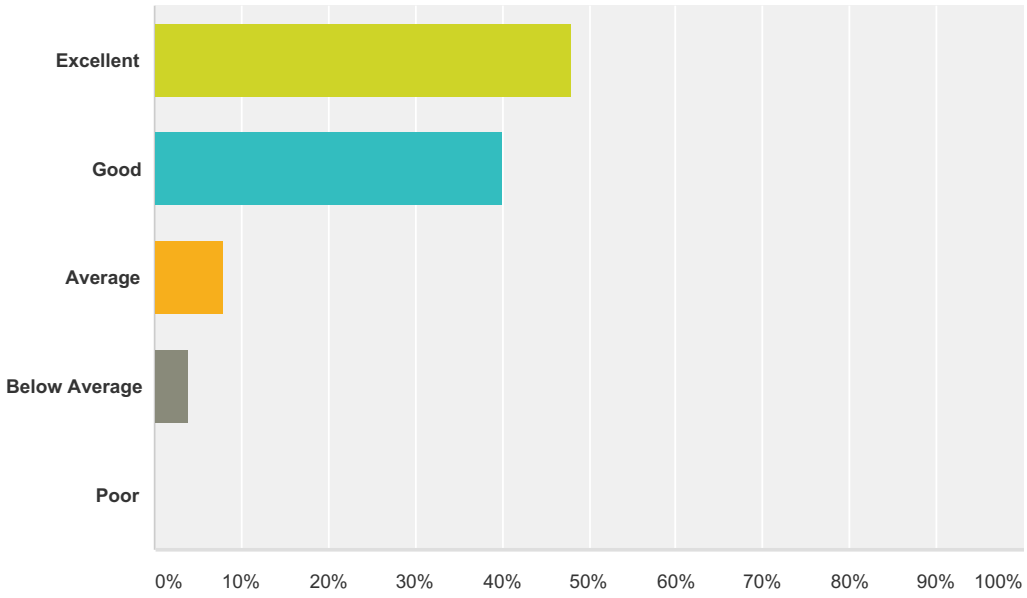
Answered: 25 Skipped: 0



Answer Choices	Responses	
Novice	**40.00%**	10
Intermediate	**56.00%**	14
Expert	**4.00%**	1
Total		**25**

Q7 How would you rate your overall experience with the morning training?

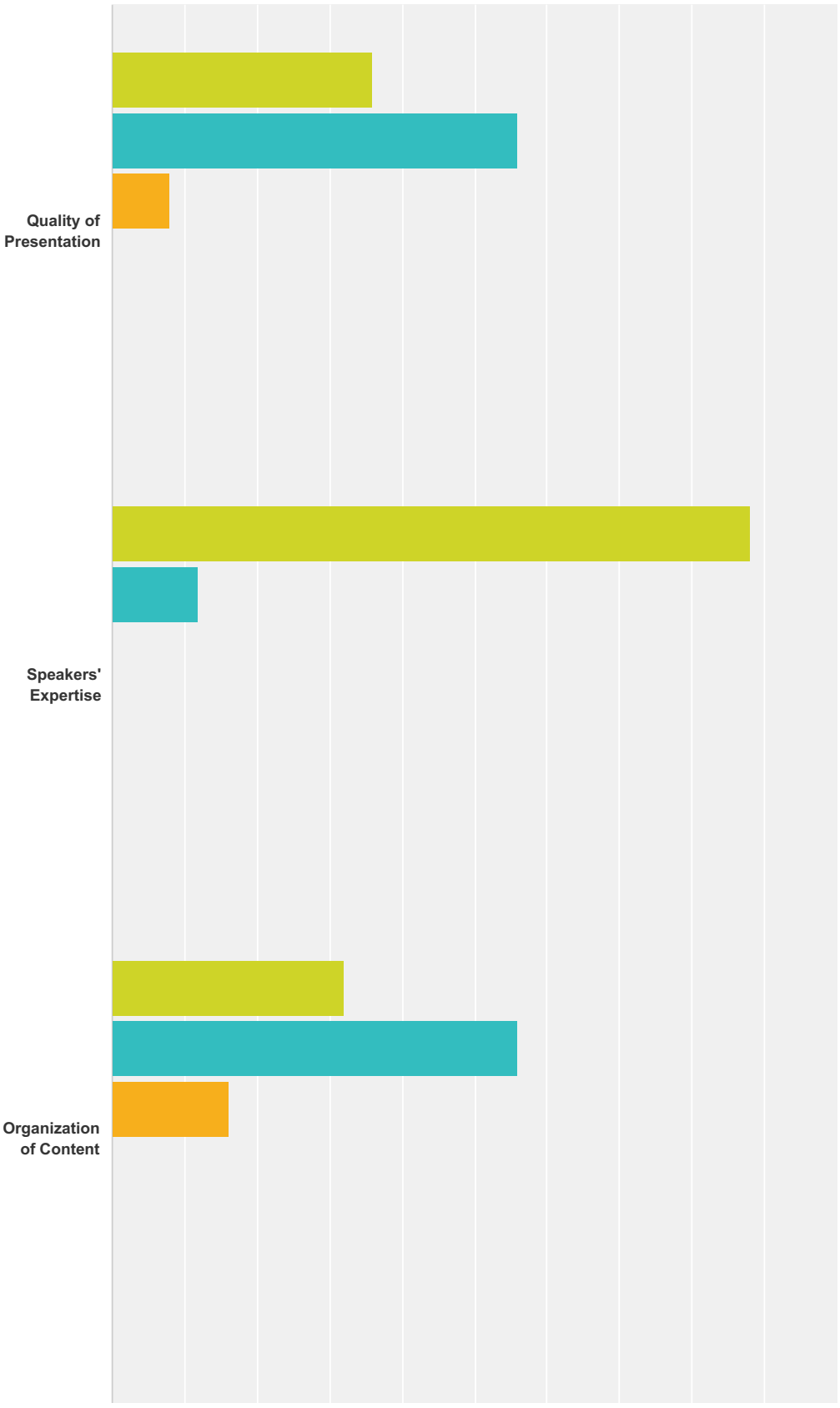
Answered: 25 Skipped: 0

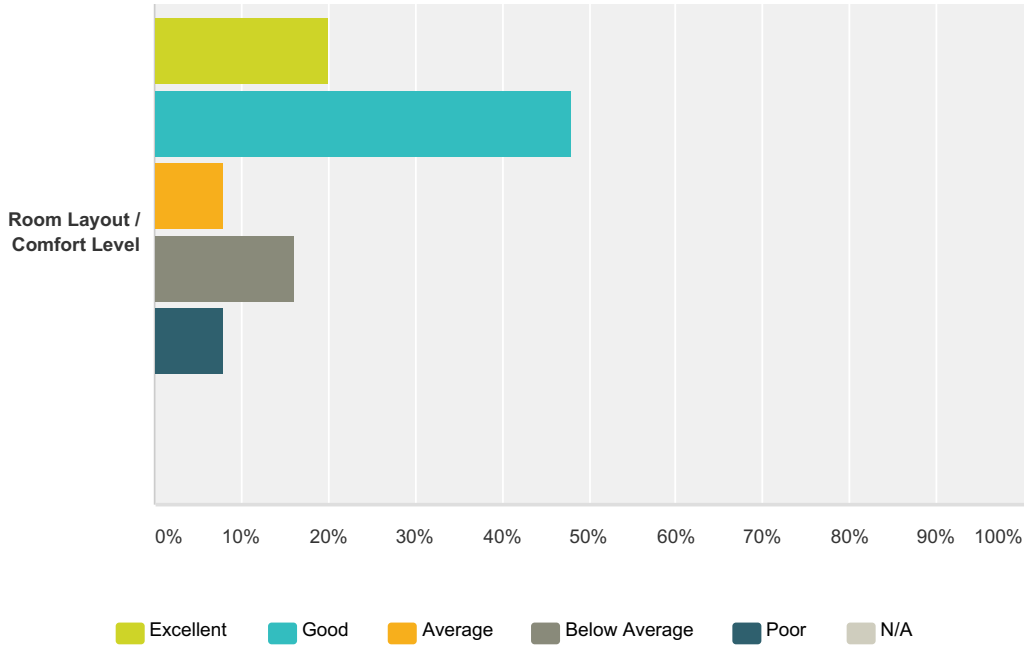


Answer Choices	Responses	
Excellent	**48.00%**	12
Good	**40.00%**	10
Average	**8.00%**	2
Below Average	**4.00%**	1
Poor	**0.00%**	0
Total		**25**

Q8 Please rate your experience with the morning training in these areas:

Answered: 25 Skipped: 0

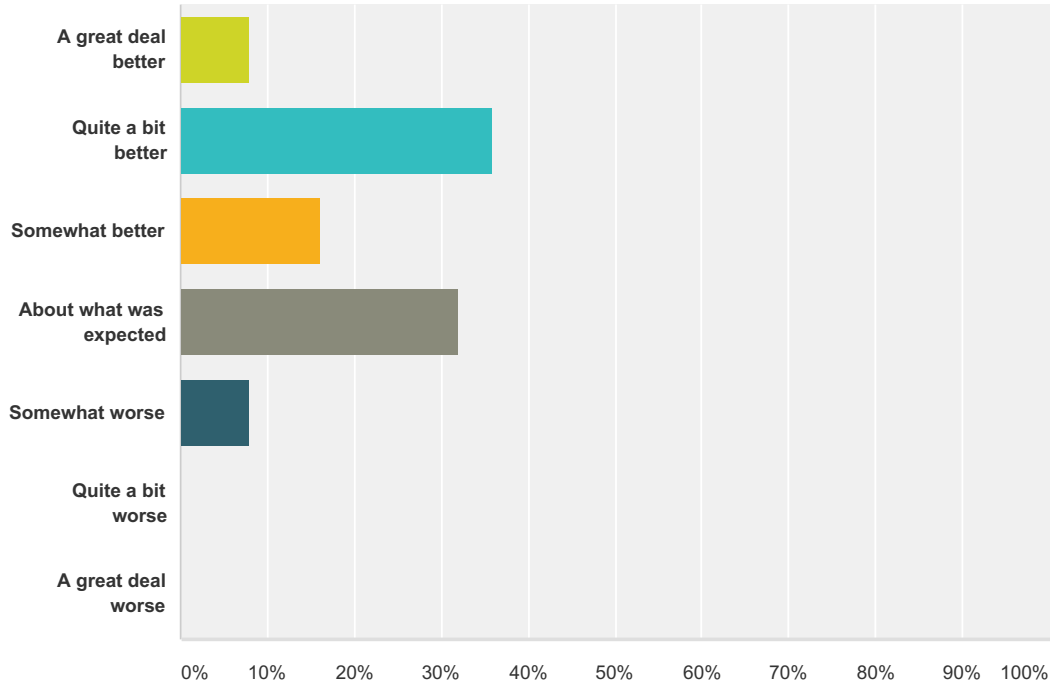




	Excellent	Good	Average	Below Average	Poor	N/A	Total Respondents
Quality of Presentation	**36.00%** 9	**56.00%** 14	**8.00%** 2	**0.00%** 0	**0.00%** 0	**0.00%** 0	25
Speakers' Expertise	**88.00%** 22	**12.00%** 3	**0.00%** 0	**0.00%** 0	**0.00%** 0	**0.00%** 0	25
Organization of Content	**32.00%** 8	**56.00%** 14	**16.00%** 4	**0.00%** 0	**0.00%** 0	**0.00%** 0	25
Room Layout / Comfort Level	**20.00%** 5	**48.00%** 12	**8.00%** 2	**16.00%** 4	**8.00%** 2	**0.00%** 0	25

Q9 Was this morning training better than what you expected, worse than what you expected, or about what you expected?

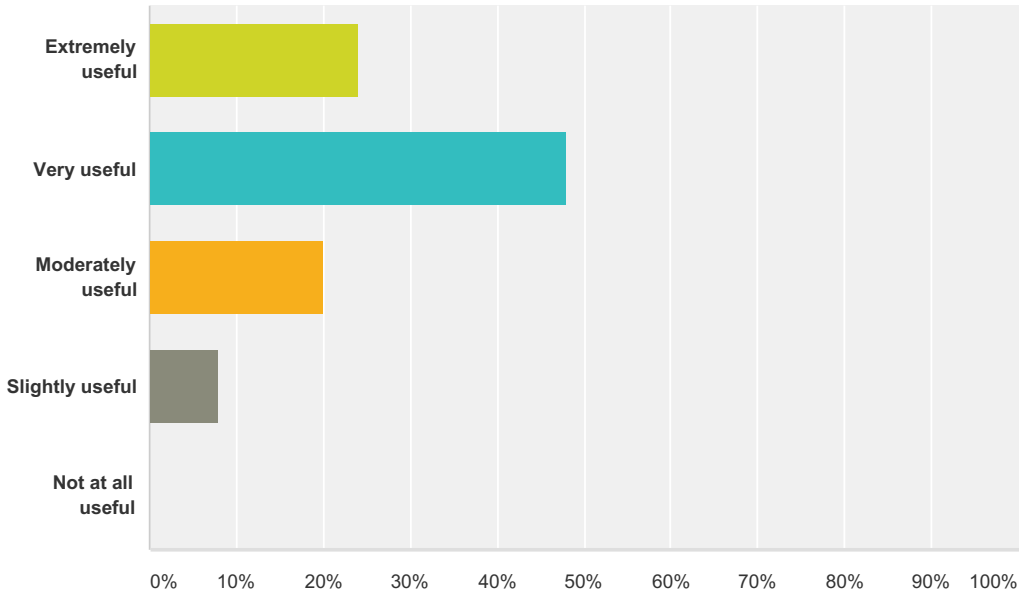
Answered: 25 Skipped: 0



Answer Choices	Responses	
A great deal better	8.00%	2
Quite a bit better	36.00%	9
Somewhat better	16.00%	4
About what was expected	32.00%	8
Somewhat worse	8.00%	2
Quite a bit worse	0.00%	0
A great deal worse	0.00%	0
Total		**25**

Q10 How useful to your work was this morning training?

Answered: 25 Skipped: 0

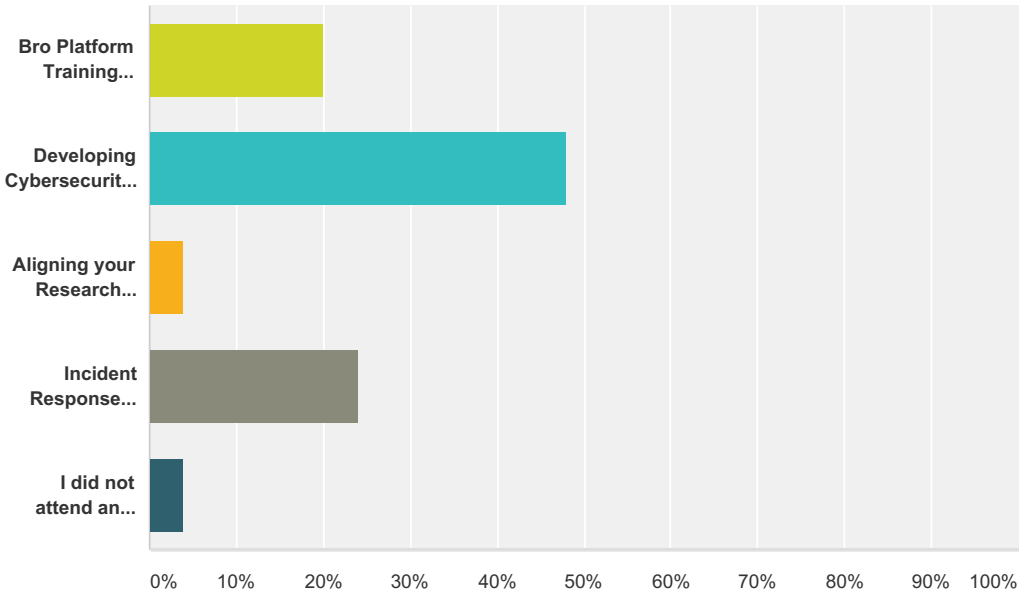


Answer Choices	Responses	
Extremely useful	**24.00%**	6
Very useful	**48.00%**	12
Moderately useful	**20.00%**	5
Slightly useful	**8.00%**	2
Not at all useful	**0.00%**	0
Total		**25**

Responses to Question 11 (How can we improve this training session in the future?) and Question 12 (Were there any aspects of the morning training you found particularly useful or important? Please explain) are open-ended responses directed at specific training sessions. They have been provided to the respective training teams, and are removed from this appendix.

Q13 Which afternoon session did you attend?

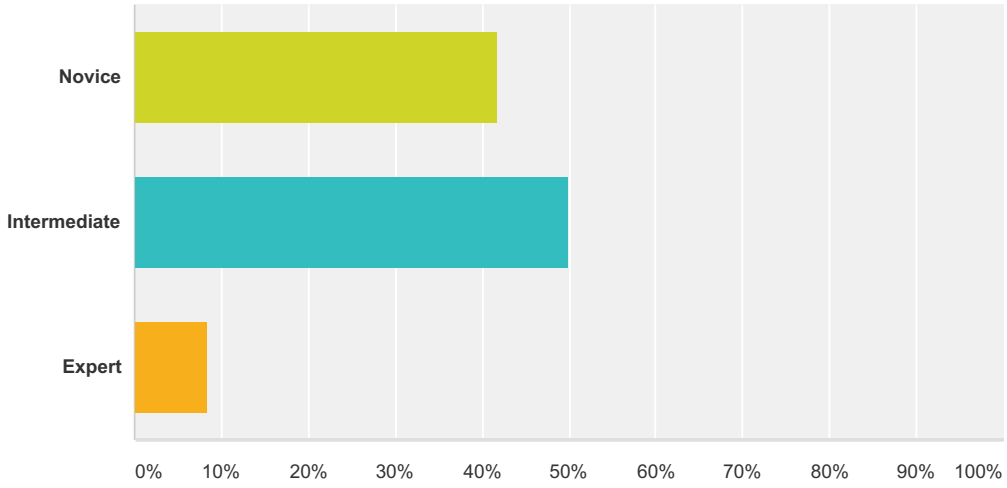
Answered: 25 Skipped: 0



Answer Choices	Responses	
Bro Platform Training Workshop (Justin Azoff, Adam Slagell & Johanna Amann)	**20.00%**	5
Developing Cybersecurity Programs for NSF Projects (CTSC Team)	**48.00%**	12
Aligning your Research Cyberinfrastructure with HIPAA and FISMA (Anurag Shankar)	**4.00%**	1
Incident Response Training (Randy Butler)	**24.00%**	6
I did not attend an afternoon session	**4.00%**	1
Total		**25**

Q14 How would you rate your level of pre-training familiarity with the topics covered by this afternoon training session?

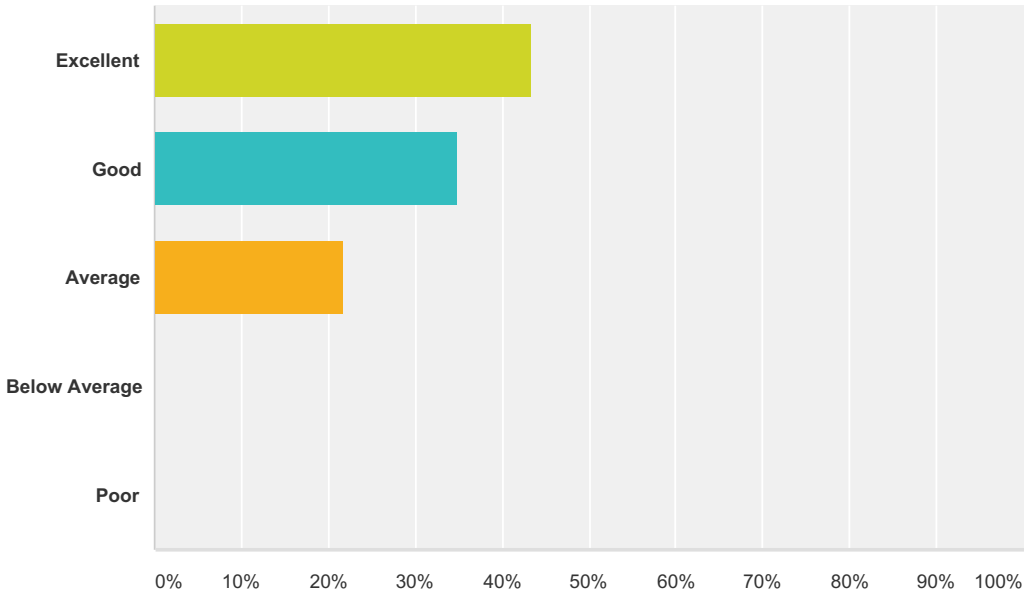
Answered: 24 Skipped: 1



Answer Choices	Responses	
Novice	**41.67%**	10
Intermediate	**50.00%**	12
Expert	**8.33%**	2
Total		**24**

Q15 How would you rate your overall experience with the afternoon training?

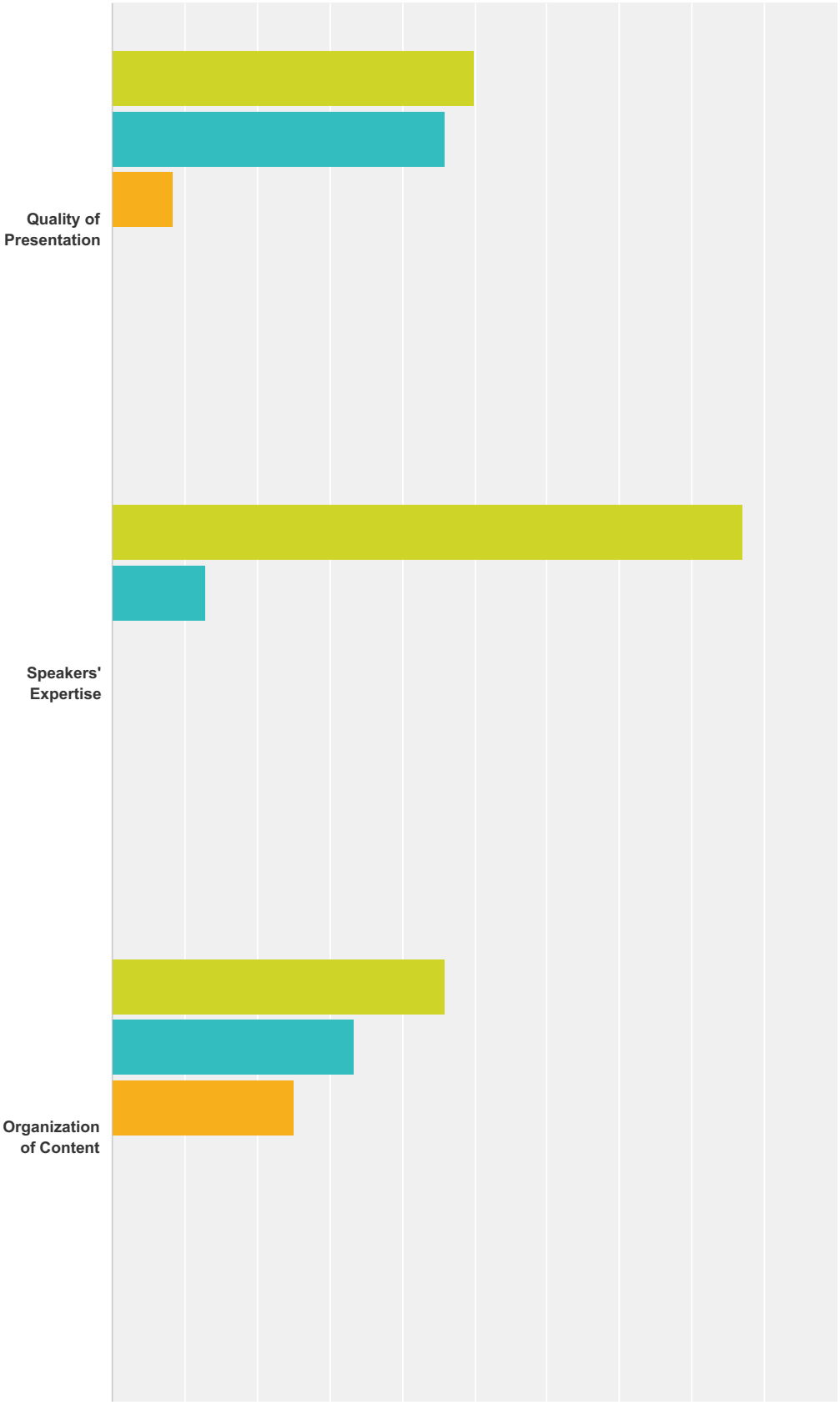
Answered: 23 Skipped: 2

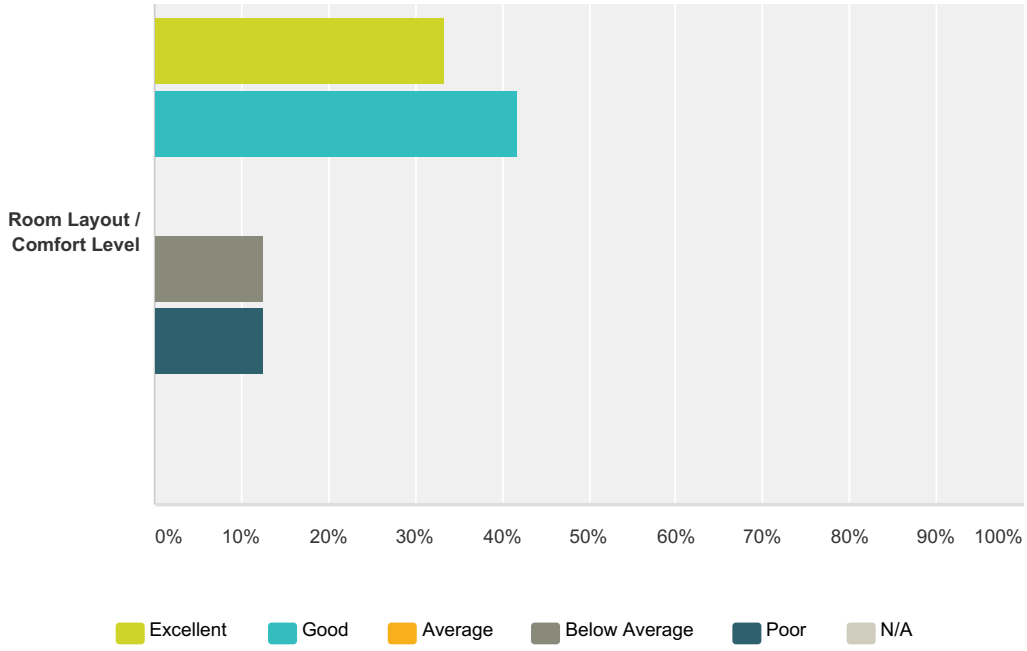


Answer Choices	Responses	
Excellent	**43.48%**	10
Good	**34.78%**	8
Average	**21.74%**	5
Below Average	**0.00%**	0
Poor	**0.00%**	0
Total		**23**

Q16 Please rate your experience with the afternoon training in these areas:

Answered: 24 Skipped: 1

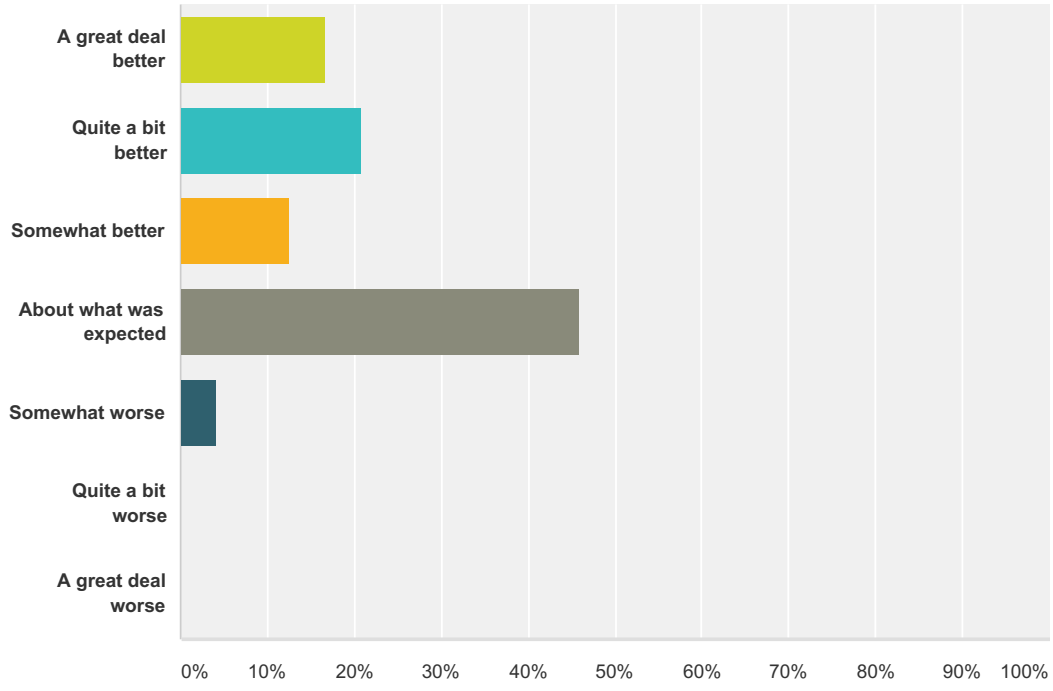




	Excellent	Good	Average	Below Average	Poor	N/A	Total Respondents
Quality of Presentation	**50.00%** 12	**45.83%** 11	**8.33%** 2	**0.00%** 0	**0.00%** 0	**0.00%** 0	24
Speakers' Expertise	**86.96%** 20	**13.04%** 3	**0.00%** 0	**0.00%** 0	**0.00%** 0	**0.00%** 0	23
Organization of Content	**45.83%** 11	**33.33%** 8	**25.00%** 6	**0.00%** 0	**0.00%** 0	**0.00%** 0	24
Room Layout / Comfort Level	**33.33%** 8	**41.67%** 10	**0.00%** 0	**12.50%** 3	**12.50%** 3	**0.00%** 0	24

Q17 Was this afternoon training session better than what you expected, worse than what you expected, or about what you expected?

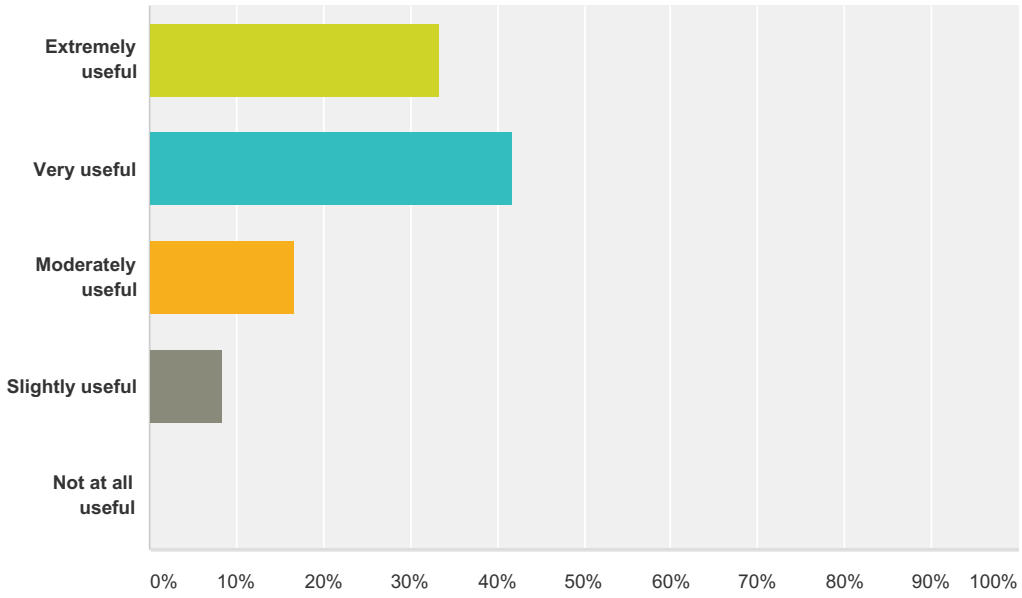
Answered: 24 Skipped: 1



Answer Choices	Responses	
A great deal better	**16.67%**	4
Quite a bit better	**20.83%**	5
Somewhat better	**12.50%**	3
About what was expected	**45.83%**	11
Somewhat worse	**4.17%**	1
Quite a bit worse	**0.00%**	0
A great deal worse	**0.00%**	0
Total		**24**

Q18 How useful to your work was this afternoon training?

Answered: 24 Skipped: 1



Answer Choices	Responses	
Extremely useful	**33.33%**	8
Very useful	**41.67%**	10
Moderately useful	**16.67%**	4
Slightly useful	**8.33%**	2
Not at all useful	**0.00%**	0
Total		**24**

Responses to Question 19 (How can we improve this training session in the future?) and Question 20 (Were there any aspects of the morning training you found particularly useful or important? Please explain) are open-ended responses directed at specific training sessions. They have been provided to the respective training teams, and are removed from this appendix.