



Report of the
2013 NSF Cybersecurity Summit for
Cyberinfrastructure and Large Facilities
Designing Cybersecurity Programs in Support of Science
September 30 - October 2
Hilton Arlington - Arlington, VA

February 5, 2014
For Public Distribution

Craig Jackson, James Marsteller, Von Welch

About CTSC

The mission of the Center for Trustworthy Scientific Cyberinfrastructure (CTSC, trustedci.org) is to improve the cybersecurity of NSF science and engineering projects, while allowing those projects to focus on their science endeavors. This mission is accomplished through one-on-one engagements with projects to address their specific challenges; education, outreach, and training to raise the state of security practice across the scientific enterprise; and leadership on bringing the best and most relevant cybersecurity research to bear on the NSF cyberinfrastructure research community.

Acknowledgments

The organizers wish to thank those all who attended the summit, whether new to this community or coming back together after a 4 year hiatus. Special gratitude goes to all who spoke and participated, those who developed and delivered tutorials, the program committee, those who took notes (Rakesh Bobba, Terry Fleury and Randy Heiland), Joel Cutcher-Gershenfeld for providing his insights though unable to attend due to an emergency, and Cliff Jacobs for providing slides despite not being able to attend due to the federal government shutdown (those individuals not listed here are identified subsequently in this document). We thank the community members who provided comments on this report, and Ardoth Hassler in particular for her considerable contributions. Our sincere thanks goes to the National Science Foundation and Indiana University's Center for Applied Cybersecurity Research for making this 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 their authors and do not necessarily reflect the view of the National Science Foundation or any other organization.

Using & Citing this Work

This work is made available under the terms of the Creative Commons Attribution 3.0 Unported License. Please visit the following URL for details: http://creativecommons.org/licenses/by/3.0/deed.en_US

Site this work using the following information:

Craig Jackson, James Marsteller, Von Welch. Report of the 2013 NSF Cybersecurity Summit for Cyberinfrastructure and Large Facilities: Designing Cybersecurity Programs in Support of Science. <https://trustedci.org/summit/>

For the latest information on the Summit:

Please visit <http://trustedci.org/summit/>

Table of Contents

Executive Summary.....	4
1 Background: Prior Summits and the Evolving NSF Cybersecurity Landscape	5
2 The 2013 NSF Cybersecurity Summit Goals and Scope	5
3 The Organizing and Program Committees	6
4 Participants	7
5 The Program	9
5.1 Theme	9
5.2 Program Changes Due to Government Shutdown.....	10
5.3 Day 1 Tutorials – September 30, 2013.....	10
5.4 Day 2 Plenary – October 1, 2013	11
5.5 Day 3 Working Groups – October 2, 2013	14
6 Findings	15
7 Attendee Evaluations.....	17
7.1 Attendee Survey	17
7.2 Tutorial Surveys	18
8 The Trusted CI Forum: Continued Community Building and Support.....	19
9 Closing Thoughts from the Organizers.....	20
References	20
Appendix A: Listing of Attendees and Organizations	
Appendix B: Agenda	
Appendix C: Bios for Speakers, Program Committee, and Organizers	
Appendix D: Handout	
Appendix E: Day 2 Contingency Agenda	
Appendix F: Attendee Survey Summary Report	
Appendix G: Tutorial Evaluation Survey Summary Report	

Executive Summary

The 2013 NSF Cybersecurity Summit for Cyberinfrastructure and Large Facilities developed around the theme, ***Designing Cybersecurity Programs in Support of Science***, with an explicit focus on the challenges of supporting the community of practitioners and stakeholders who must secure scientific CI. Despite falling on the first day of the government shutdown, preventing attendees from NSF from participating, sixty-nine (69) people attended the summit, representing 24 NSF-funded projects and 30 organizations.

The Summit spanned three days. The first day offered tutorials on four subjects (identity management, network security and monitoring, cybersecurity planning, and secure software development). Day 2 was in plenary, tackling the Summit's theme of Designing Cybersecurity Programs in Support of Science. Day 3 had the participants breaking out into working groups to tackle specific technical areas. Efforts by the working groups continue in the Trusted CI Forum (trustedci.groupsites.com), an online community established to support continuing collaboration regarding cybersecurity by the NSF community.

The following findings resulted from the Summit presentations, discussions and/or evaluation feedback:

1. The community should identify a means to organize future summits.
2. Future summits should continue to include NSF project principal investigators, other key stakeholders, and risk owners to ensure that NSF cybersecurity evolves to address their needs.
3. Future program committees should consider more time and opportunities (*e.g.*, increased seating) for tutorials, hands-on activities, and organized discussion.
4. 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.
5. The community should consider the cybersecurity needs of and relationship between large facilities and smaller cyberinfrastructure projects, as well as how (and if) the summit can effectively address both.
6. The community needs to develop a better understanding of the expectations for their cybersecurity programs and how to meet those expectations.

1 Background: Prior Summits and the Evolving NSF Cybersecurity Landscape

Spanning six years from 2004-2009, the NSF-funded annual cybersecurity summits served as a valuable part of the process of securing the NSF-funded cyberinfrastructure (CI) and MREFC projects by providing the community with the opportunity to share best practices, educate themselves from experts both from within and from outside of the community, and collaborate on solving common challenges. The first summit was a response to the widespread unauthorized intrusions of 2003 - 2004 that affected many communities including NSF-funded cyberinfrastructure. Since then, the cybersecurity needs of NSF communities have driven the agenda and program content. Feedback from the 2009 summit [1] was very positive and showed a strong desire by the community for future events. In 2010 and 2011, two Scientific Software Security Innovation Institute workshops, which included representatives of 35 MREFC and major NSF-funded cyberinfrastructure projects, indicated that leadership and guidance are still high priority needs of the community in the area of cybersecurity [2].

Since the last summit in 2009, the threat landscape for both the Internet and NSF CI has continued to evolve and become more complex, as discussed on Day 2 of the summit by Adam Slagell (*see*, Section 5.4), with an increasing variety of threat actors and increasingly targeted attacks on information resources. Though attention to cybersecurity is a well-established necessity, the realities of limited budgets and resources to address these concerns have become ever starker. During this time the community has been without a venue to interact as a community, share experiences, and collectively ascertain the impact of the evolving information security threats to NSF CI (*e.g.*, threats to scientific data integrity and unique science instruments).

2 The 2013 NSF Cybersecurity Summit Goals and Scope

In 2012, the NSF funded the Center for Trustworthy Scientific Cyberinfrastructure¹ (CTSC) to help the NSF community tackle cybersecurity challenges. CTSC's broader mission is to improve the cybersecurity of NSF science and engineering projects, while allowing those projects to focus on their science endeavors. As one of CTSC's major leadership initiatives, it sought to

¹ <http://trustedci.org>

reestablish the NSF cybersecurity summits as initial step toward reinvigorating the NSF cybersecurity community.

With the history described in the previous section in mind, the 2013 NSF Cybersecurity Summit developed around the theme, ***Designing Cybersecurity Programs in Support of Science***. This theme suggested a number of challenges to be addressed: How do we build a community for sharing experiences and supporting continuity between projects? What are the goals of a cybersecurity plan for the vast variety of NSF projects; what are the key motivations, assets and threats? How are we similar to and different from other communities addressing cybersecurity (*e.g.*, higher education, government, private sector), and how do we relate to them?

This summit's scope was explicitly extended to encompass not only NSF large facilities and MREFCs, but other cyberinfrastructure projects as well. The large facilities and other projects, as shown by the events in 2003-2004, often tie into broader collaborations with their security interconnected.

The remainder of this report outlines the summit organizational process, details on attendance and participation, the resultant program and highlights from the various sessions, findings of the Summit, and results of attendees' evaluations of the event. The report closes with a discussion of efforts to support continuity of this community from year to year, and closing thoughts of the organizers.

3 The Organizing and Program Committees

The Summit was funded largely by a supplemental grant to the CTSC project, and three members of that project (Craig Jackson, James Marsteller, and Von Welch) acted as an organizing committee with responsibility for the Summit. Their first act was to organize a program committee (PC) comprised of community leaders both cognizant of NSF's cybersecurity needs and activities in the broader cybersecurity domain and welcoming of the responsibility for setting the specific agenda and inviting speakers. Marsteller filled a role he held in prior Summits as chair of the program committee.

The 2013 PC members are:

- **Michael Bailey**, Associate Research Professor, LEO Adjunct Lecturer, and Co-Director of the Network and Security Research Group, University of Michigan
- **Scott Campbell**, Security Team, LBNL/NERSC
- **Michael Corn**, Chief Information Security Officer, University of Illinois, and Chief Privacy and Security Officer, University of Illinois at Urbana-Champaign (now serving as Deputy CIO and CISO at Brandeis University)
- **Deborah A. Frincke**, Deputy Director for Research, National Security Agency
- **Ardoth Hassler**, Associate Vice President of University Information Services & Executive Director, Office of Assessment and Decision Support, Georgetown University
- **Craig Jackson** (Organizer), Project Manager / Policy Analyst, Center for Applied Cybersecurity Research, Indiana University, and Center for Trustworthy Scientific Cyberinfrastructure (CTSC)
- **James A. Marsteller** (Organizer and Program Committee Chair), Information Security Officer, Pittsburgh Supercomputing Center, and Co-PI, Center for Trustworthy Scientific Cyberinfrastructure (CTSC)
- **Rodney J. Petersen**, Managing Director of Washington Office and Senior Government Relations Officer, EDUCAUSE
- **Mark Servilla**, Lead Scientist, Network Information System, LTER Network Office
- **Von Welch** (Organizer), Deputy Director, Center for Applied Cybersecurity Research, Indiana University, and PI, Center for Trustworthy Scientific Cyberinfrastructure (CTSC)

The PC undertook 4 core tasks: (1) Evaluate and set the theme for the 2013 Summit; (2) set the program agenda; (3) recommend and assist in recruiting speakers and discussion leaders; and (4) assist in ensuring we target an appropriate range of invitees. The PC held weekly, 1-hour phone calls beginning June 21, 2013 and ending July 31, 2013, and conferred electronically both before and following this time period.

4 Participants

As with prior summits, the 2013 summit was an invitation-only event, with no fee to attend. Invitations went to PIs and those with cybersecurity responsibility in MREFCs, CI infrastructure projects, SI2 awardees, and other NSF-funded CI projects. In general, we sought to be inclusive of anyone in the community with interest and grounds for attending, and accepted delegated

registrations when they arose. We also extended invitations to select individuals from outside the NSF community (*e.g.*, Department of Energy, Internet2, higher education) to avoid being insular and to add context.

In our summit agenda, we described the ideal summit attendee as follows:

The ideal summit attendee can speak to the needs of the science mission of their project or community has for cybersecurity, as well as the social, human resource, policy and other challenges for creating a cybersecurity program that leaves their community comfortable those needs have been met.

Ninety-nine individuals registered for the summit. However, due largely to a federal government shutdown² looming on Day 1 and in effect for Days 2 and 3 of the summit, thirty (30) registered individuals did not participate at all. At least twenty-six (26) of those thirty individuals were from NSF and were prohibited from participating. Altogether, sixty-nine (69) attendees (including speakers, tutorial presenters, panelists, program committee) participated in some part of the summit. A listing of the attendees and their affiliations is included as Appendix A. Thirty-one (31) of those 69 participated in planning, spoke, provided training, and/or led a breakout group.

The following numbers break down attendance by the day:

- Fifty-eight (58) attendees participated in the Day 1 tutorials. These sessions were popular during registration, with all but one session reaching capacity.
- Sixty (60) attendees attended the Day 2 plenary.
- Forty-four (44) attendees from Day 2 remained with us and participated in the working groups on Day 3.

The following NSF-funded projects were represented at the summit:

1. Bro Center of Expertise
2. Center for Trustworthy Scientific Cyberinfrastructure (CTSC)
3. Cornell Laboratory for Accelerator-based ScienceS and Education (CLASSE)
4. Data Observation Network for Earth (DataONE)
5. Extreme Science and Engineering Discovery Environment (XSEDE)
6. Global Environment for Network Innovations (GENI)
7. HUBZero
8. IceCube South Pole Neutrino Observatory (IceCube)

² http://en.wikipedia.org/wiki/United_States_federal_government_shutdown_of_2013

9. Integrated Ocean Drilling Program (IODP)
10. International Computer Science Institute (ICSI)
11. Laser Interferometer Gravitational-Wave Observatory (LIGO)
12. Long Term Ecological Research Network (LTER)
13. National Center for Atmospheric Research (NCAR)
14. National Center for Supercomputing Applications (NCSA)
15. National High Magnetic Field Laboratory (Magnet Lab)
16. National Institute for Computer Sciences (NICS)
17. National Radio Astronomy Observatory (NRAO)
18. National Solar Observatory (NSO)
19. National Superconducting Cyclotron Laboratory (NSCL)
20. Network for Earthquake Engineering Simulation (NEES)
21. Open Science Grid (OSG)
22. Pittsburgh Supercomputing Center (PSC)
23. San Diego Supercomputer Center (SDSC)
24. Texas Advanced Computing Center (TACC)

5 The Program

The full agenda, biographies, one-page handout, and revised Day 2 agenda are Appendices B, C, D, and E. The full summit program is also available on the CTSC website, <http://trustedci.org/summit/>. A one-page paper handout was made available to attendees on site with the full agenda and speaker biographies available electronically (to save paper and printing costs).

5.1 Theme

The selected theme for the 2013 NSF Cybersecurity summit was ***Designing Cybersecurity Programs in Support of Science***. This theme suggested a number of challenges to be addressed: How do we build a community for sharing experiences and supporting continuity between projects? What are the goals of a cybersecurity plan for the vast variety of NSF projects; what are the key motivations, assets and threats? How are we similar to and different from other communities addressing cybersecurity (e.g., higher education, government, private sector), and how do we relate to them?

5.2 Program Changes Due to Government Shutdown

Due to the federal government shutdown, several speakers, panelists, and moderators, primarily from NSF, were unavailable. In consultation with NSF, the decision was made ahead of time to proceed with the summit. The organizers created a revised Day 2 agenda and circulated it that morning. The Day 3 program was unaffected.

5.3 Day 1 Tutorials – September 30, 2013

Attendees of prior summits reacted very positively to opportunities to develop practical technical knowledge and skills. Therefore, Day 1 offered a half-day for tutorials across key cybersecurity domains, with the CTSC personnel involved in providing three tutorials and the Bro team providing a fourth. Three of the four tutorials filled to physical capacity during pre-registration, and several attendees expressed the desire both for longer tutorial sessions and opportunities to attend additional tutorials. Descriptions are provided for each tutorial; attendance and evaluations are discussed further in later sections of this report.

Building a Cybersecurity Program (Jim Marsteller, Patrick Duda, and Rakesh Bobba)

Description: This tutorial will provide principal investigators, project leaders, and project managers planning, building and operating scientific cyberinfrastructure with a method for accessing their security needs, documenting an action plan for addressing those needs, and quantifying resource requirements. Specifically, this tutorial will provide an overview and process for developing a cybersecurity plan for scientific computing projects. Discussion will focus on why security is crucial to an organization and things that senior management can do to establish a proactive stance on cybersecurity. This tutorial will present an overview of security issues that face NSF cyber infrastructure projects. The intent is to give PI's and managers an understanding of these issues and tools to address them.

Secure Coding Practices (Prof. Barton Miller and Prof. Elisa Heymann)

Description: Security is crucial to the software that we develop and use. With the growth of both Grid and Cloud 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. 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 presents coding practices subject to vulnerabilities, with examples of how they commonly arise, techniques to prevent them, and exercises to reinforce them. Most examples are in Java, C, C++, Perl and Python, and come from real code belonging to Cloud and Grid systems we have assessed. This tutorial is an outgrowth of our experiences in performing vulnerability assessment of critical middleware, including Google Chrome, Wireshark, Condor, SDSC Storage Resource Broker, NCSA MyProxy, INFN VOMS Admin and Core,

and many others.

Streamlining Collaboration with InCommon and Identity Federations (Warren G. Anderson and Dr. Jim Basney, presenting materials developed by Scott Koranda)

Description: Because of the success of programs like XSEDE and OSG more and more scientists have access to more computing power than ever and consequently are generating more output than ever before. Efficiently sharing all those generated results with colleagues and collaborators, however, remains a problem--it's too difficult for scientists from different projects and different campuses to quickly and easily find spaces to collaborate. One of the largest barriers to efficient collaboration is creating and managing new electronic identities for every new tool or web application. Federated identity can help and identity federations like InCommon in the US provide ready to consume identities that help streamline getting scientists into the same applications and spaces so they can collaborate. This tutorial will discuss what are federated identities, why we can trust them, and how to leverage a federation like InCommon and similar federations around the world to support discovery across VOs. We will focus on LIGO's experiences and lessons learned during their five year effort to build an end-to-end identity management infrastructure that consumes federated identity in support of collaboration with other astronomy and astrophysics projects.

Bro Network Intrusion Detection (Seth Hall, Sam Oehlert, Dr. Adam Slagell, and Robin Sommer)

Description: Bro is a stateful, protocol aware open source high speed network monitor with applications as a next generation intrusion detection system, real time network discovery tool, historical network analysis tool, real time network intelligence, and dynamic active response. Originally developed by Vern Paxson, he now leads the core team of developers/researchers at both the International Computer Science Institute in Berkeley, CA and the National Center for Supercomputing Applications in Urbana-Champaign, IL. Bro provides a security team with logs of highly structured data about their network, a turing complete scripting language through which they can interact with real time stateful network events, and flexible open interfaces through which Bro can be programmed. Pragmatically able to interface with the entire network stack, Bro includes support for IPv6, tunneled traffic, SSL and more. In this presentation we present multiple case studies and are releasing their corresponding Bro scripts with source.

Day 1 concluded with a networking event for the Program Committee, tutorial presenters, speakers, and panelists.

5.4 Day 2 Plenary – October 1, 2013

Due to the federal government shutdown, Day 2 went forward under a contingency agenda (see, Appendix E). Below we highlight key content and discussion from Day 2.

Welcome and Goals (Jim Marsteller)

- Jim Marsteller kicked off the summit welcoming the attendees and delivered a brief prologue. This included establishing the theme of the summit ***Designing Cybersecurity Programs in Support of Science*** along with the vision and goals for the current and future summits. Marsteller introduced the Trusted CI Forum website as a collaborative tool intended to facilitate developmental efforts beyond the summit, to share ideas and tackle common challenges shared by the community.
- Marsteller presented comments that Cliff Jacobs prepared in advance of the federal government shutdown conveying the NSF's support for the summit and the community effort it embodies. Jacobs intended to address the community at this point in the program, but regrettably he was unable to attend.

Opening Keynote (Vern Paxson)

- Vern Paxson addressed community building with the Bro community as a case example. Paxson discussed the goals of community building around the concepts of synergy, common goals, momentum, and identity. He offered cautions and realism about community building: Community success involves a network effect, including luck. The work of a few individuals can be critical to community success, or be so disruptive as to derail the community effort.

Panel and Discussion on Community Building: Real World Experiences from Communities

- Panelists: Joel Cutcher-Gershenfeld, Jim Marsteller, Michael McLennan, Leif Nixon, Rodney Petersen
- Moderator: Craig Jackson
- Points of Discussion:
 - Community structures make the biggest impact: Opportunities to interact face-to-face in building relationships and trust, as well as support structures that collect, curate, and present the most important community information.
 - Successes and challenges in sharing cybersecurity information.
 - How to think about the make-up of our community, including the diffuse nature of contributors, users, and various stakeholders.
 - Joel Cutcher-Gershenfeld was unable to attend the panel due to an emergency situation, but provided slides and commentary which have since been shared with the community through the Trusted CI Forum.

Panel and Discussion on the Goals of a Cybersecurity Program

- Panelists: Brian Bockelman, Ardoth Hassler, John Towns
- Moderator: Von Welch
- Points of Discussion:
 - That different projects, at varying scales and with diverse assets, have very different cybersecurity needs. There is no one-size-fits-all cybersecurity program for science.
 - How to communicate the goals and value of the cybersecurity program to the scientists who represent our stakeholders. Are we doing good work, but not marketing it well?
 - The potential that the cybersecurity community shares too little, and should reset its approach to sharing from a more holistic risk management perspective.

A View from the Field of NSF Cybersecurity: Challenges, Goals, and Opportunities (Von Welch, CTSC PI)

- Von Welch gave an overview of Center for Trustworthy Scientific Cyberinfrastructure (CTSC) experiences from its first year. He discussed challenges of a complex environment, lack of simple guidance, and shared experiences and lessons learned. Welch highlighted that CTSC is providing training, one-on-one engagements, and broader leadership in developing methodologies for NSF CI cybersecurity.

Panel and Discussion on Differences, Similarities and Relationships between NSF Projects and Other Organizations (e.g., higher education, government, private sector)

- Panelists: Michael Bailey, Michael Corn, Vic Thomas
- Moderator: Greg Bell
- Points of Discussion:
 - Whether the NSF community is or is not truly unique when it comes to cybersecurity needs, and what qualities (highly distributed/collaborative community, unique instruments and CI) may give rise to that uniqueness.
 - The relationship between NSF CI projects and higher education institutions was highlighted as particularly important, and an area for future work, particularly regarding the possibility of standardizing best practices for how to formalize those relationships, as well as ensuring cybersecurity support for smaller projects without the ability to resource dedicated cybersecurity personnel.

Evolution of Network Security Threats and Capabilities for Science Communities (Adam Slagell)

- Adam Slagell discussed the changing threat landscape and its implications for NSF CI. Not only are cyber threats growing in public awareness, but we now know that no organizations get a “free pass” on cybersecurity. The risk of cybercrime, particularly cybercrime utilizing botnets, and digital/virtual currencies mean that entities with significant computing power are more desirable targets. Slagell also had the opportunity to announce the Bro Center of Expertise, funded by the National Science Foundation (NSF) as a central point of contact for institutions that bundles the Bro Team’s expertise and offers it to NSF-supported sites seeking advice.

Day 2 concluded with an optional informal gathering of attendees for dinner. Approximately two dozen people attended and conversations both continued discussions from the Summit as well as branched out into related topics.

5.5 Day 3 Working Groups – October 2, 2013

A long-term goal for the summit and CTSC is to build and support community that spans from year to year. Therefore, summit attendees were invited to join one of three half-day working groups. (A fourth open-ended “unconference” working group was offered, but interest in the other three and lack of strong support for a fourth topic meant that it was unnecessary.) The primary goal for each group was to define a problem statement or charter around the working group topic to serve as a basis for collaboration after the 2013 summit, and feed into the anticipated 2014 summit. Participants were given the opportunity to join dedicated groups in the Trusted CI Forum (trustedci.groupsite.com) to continue working together. In support of this goal, possible Day 3 objectives for each group included (a) identifying the most critical and vexing questions for making progress in the topic area, (b) identifying resources and expertise that can be leveraged to address these challenges, and (c) identifying ways to usefully build community and communication around the topic area.

Cybersecurity Planning & Programs: Jim Marsteller (discussion leader), Randy Heiland (reporter)

- Discussed AUPs, audits, leveraging parent organization policies and resources, and the variety of information assets and security concerns that require special consideration when developing cybersecurity programs for NSF CI. An overarching theme of discussion was how to achieve pragmatic levels of security, appropriate to the scope and resources of science projects.

- Laid out plans and identified team leaders to use Trusted CI Forum to work on the following areas of focus:
 - Share/compare local cybersecurity policies and develop a template/sample cybersecurity policy for the CI community.
 - Identify common CI project risks and threats
 - Define how CI projects are different from other information technology environments.
 - Develop a consensus on cybersecurity terminology.

Network Security & Monitoring: Robin Sommer and Adam Slagell (discussion leaders), Rakesh Bobba (reporter)

- Discussed issues around asset management and data analytics for security.
- Considered use of Trusted CI Forum as a curated forum for scripts, tools, and documentation for getting started with Bro and other NSM tools.

Identity & Access Management: Jim Basney (discussion leader), Terry Fleury (reporter)

- Discussed and compiled a number of “unmet needs” in the identity management space.
- Identified next steps for participants in this working group including participation in InCommon Assurance and InCommon Interfederation groups; and OSG, TACC, and NCSA/CTSC to participate in a community group for IdM around campus compute clusters.

6 Findings

The following findings resulted from the summit presentations, discussions and/or evaluation feedback:

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

Discussion: The Summit was well-attended and highly-rated. Anecdotal conversations with attendees indicated a pent-up demand for continued interactions.

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

Discussion: Ultimately NSF cybersecurity programs must serve not only practitioners of cybersecurity, but their projects’ stakeholders (PIs and others who own risks associated

with threats) and ultimately the broader community (e.g., scientists, NSF).

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

Discussion: The tutorials were space limited. Evaluations both rated them highly and requested more tutorials (and more hands-on tutorials specifically).

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

Discussion: The lack of such diversity at the summit was objectively apparent and pointed out by several attendees.

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

Discussion: This was the first time a summit's scope was explicitly broadened beyond large facilities. From evaluation feedback, it was clear this created a little confusion. There was also discussion about the degree of consistency of cybersecurity needs across this larger community and if the summit might be taking on too much.

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

Discussion: The strong demand for the training, the evaluation responses, and several discussions all indicate that the community is still not certain what the expectations are for a cybersecurity program or how they go about fulfilling those expectations. From some discussions and evaluation responses, it is clear there is a subset of the community that expects NSF to provide greater clarity, while others believe we can make progress as a community.

7 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 four Day 1 tutorials.

7.1 Attendee Survey

A summary of the general survey results is included as Appendix F. We summarize the results of the general survey below.

Forty-one (41) attendees (approximately 60% 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 largely favorable. Selections follow:

- To Question #5, “How would you rate your overall experience with the 2013 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 exceeded or met the expectations of 92.6% of respondents, including 36.6% percent of respondents selecting that it was “Quite a bit better” than expected.
- To Question #8, “How useful to your work was the information discussed at the summit?,” 95.2% of respondents gave ratings of “moderately useful” to “extremely useful.”
- To Question #10, “Would you like to attend future summits?,” 85.4% responded “Yes,” with the remaining 14.6% responding “Maybe.”

Questions 11 and 12 asked for 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 11 asked “How can we improve the summit experience in the future?”
 - Of the 24 respondents, 6 suggested more training or “hands on” opportunities would improve future summits.
 - Two respondents identified the lack of gender, age, and/or racial/ethnic diversity among the attendees. This was also a point of discussion during the Day 2 plenary session. We have identified increased diversity as a strategic goal for future summits.
 - Three respondents complained specifically that a few individuals dominated discussion opportunities, two of which indicated a better job could be done in the moderation of these discussions. Because we also note that discussion moderation is a skill, we are considering how we might resource moderation expertise or training for future events. (It is worth noting that this was a community building challenge mentioned by Paxson in his keynote.)
 - At least two comments indicated greater clarity was needed with regard to the summit’s scope and addressing both large facilities and smaller projects.
- Question 12 asked “Were there any aspects of the summit you found particularly useful or important? If so, please explain.”
 - Of the 23 respondents, 9 in some fashion highlighted networking and/or opportunities meet, interact with, or compare notes with peers as particularly useful or important. Three (3) additional respondents specifically singled out the Day 3 working group.

7.2 Tutorial Surveys

The responses to the tutorial-specific surveys were very positive, and included constructive feedback. The aggregated ratings in Questions 1 through 7 are attached as Appendix G. We summarize a few aggregate responses below:

- To Question 3, “How would you rate your overall experience with the tutorial?,” 21 of 22 respondents rated their tutorial experience as Good or Excellent, with over half of selecting Excellent.
- To Question 5, “Was this tutorial better than what you expected, worse than what you expected, or about what you expected?,” the tutorial met or exceeded the expectations of 95.5% of respondents.
- To Question 6, “How useful to your work was the tutorial?,” 77.3% rated their tutorial as Very Useful for Extremely Useful.
- To Question 7, “Based on your experience, would you participate in tutorials offered at future summits?,” 86.4% responded “Yes.”

The responses for the individual tutorials were filtered and reported back to their respective tutorial leaders, including responses to Question 8, “How can we improve this tutorial in the future?” and Question 9, “Were there any aspects of the tutorial you found particularly useful or important? Please explain.”

8 The Trusted CI Forum: Continued Community Building and Support

The organizers’ vision is to build and sustain a community over multiple years; to build an increasing knowledge set from year-to-year; to retain that knowledge and know-how despite individuals entering and leaving the community; and to provide new projects with a basis to begin learning about NSF CI cybersecurity.

To that end, the Trusted CI Forum (trustedci.groupsie.com) was launched in the weeks leading up to the summit as part of an effort to build and support community in the wake of this summit and from year-to-year. The purpose and audience are stated as follows: “This forum is for discussion of cybersecurity of cyberinfrastructure supporting computational science. It is open to any member of a NSF project or member of the higher education community with an interest in cybersecurity for NSF cyberinfrastructure.” As of February 5, 2014, the Trusted CI Forum has 72 members.

9 Closing Thoughts from the Organizers

The summit was very well received. Attendees particularly valued the Day 1 tutorials and the various opportunities to interact with colleagues in the community. We would again like to thank the program committee, speakers, and other participants in making the summit a success. We noted a high level of energy and engagement throughout the event, with attendees readily asking questions and sharing ideas. Specific to CTSC, the summit was a valuable opportunity to make new connections, with at least two new engagements getting their start in the halls of the Hilton Arlington.

The presentations made clear that building community structures and supporting community processes to share cybersecurity experiences and best practices is a non-trivial task, and will require both time/effort and a shift in thinking about openness. While there is pent-up energy in the community, there is also a tradition of caginess about sharing cybersecurity information. We are cautiously optimistic about the Trusted CI Forum as a community structure to bridge from year to year, and see it as working well thus far for the Cybersecurity Planning and Programs working group.

Our hope is to follow this summit with another in 2014; we are excited about working to make that happen.

References

- [1] 2009 Cybersecurity Summit Report, <http://net.educause.edu/ir/library/pdf/PUB1001.pdf>
- [2] Butler, R., V. Welch, J. Basney, S. Koranda, W.K. Barnett and D. Pearson. Report of NSF Workshop Series on Scientific Software Security Innovation Institute. 2011. Available from: <http://hdl.handle.net/2022/14174>

Appendix A
Listing of Attendees and Organizations

Appendix A. Listing of Attendees and Organizations

Last Name	First Name	Organization Provided
Anderson	Warren	LIGO - UWM
Arshad	Fahad	Purdue University/NEES
Bagchi	Saurabh	Purdue University/NEES
Bailey	Michael	University of Michigan
Barnet	Steve	UW-Madison - IceCube
Barton	Tom	University of Chicago
Basney	Jim	CTSC / NCSA
Beaty	Steve	NCAR
Behr	Steve	National Superconducting Cyclotron Laboratory
Bell	Greg	Lawrence Berkeley National Laboratory
Bobba	Rakesh	University of Illinois
Bockelman	Brian	Open Science Grid
Boldischar	Michael	University of Minnesota
Campbell	Scott	LBNL/NERSC
Corn	Michael	University of Illinois at UIUC
Dooley	Rion	TACC
Duda	Patrick	NCSA
Epstein	Jeremy	NSF [attended Sep 30 only]
Filus	Shane	PSC
Fleury	Terry	CTSC / NCSA
Gates	Phil	Integrated Ocean Drilling Program
Giardina	Dwayne	LIGO - CA Institute of Technology
Goodrich	Bret	National Solar Observatory
Hacker	Thomas	Purdue University
Hall	Seth	International Computer Science Institute
Halstead	David	NRAO
Hanks	Jonathan	LIGO Hanford Observatory / California Institute of Technology
Hassler	Ardoth	Georgetown University
Heiland	Randy	Indiana University
Heymann	Elisa	University Autonomo of Barcelona
Jackson	Craig	Indiana U.
Jacobs	Cliff	NSF [attended Sep 30 only]
Jensen	Peter	National High Magnetic Field Laboratory
Klingenstein	Ken	Internet2

Landwehr	Carl	George Washington U
Marsteller	James	PSC/CMU
McLennan	Michael	HUBzero / Purdue University
Mendoza	Nathaniel	TACC
Miller	Bart	University of Wisconsin
Munoz	Jose	NSF [attended Sep 30 only]
Murphy	Patrick	National Radio Astronomy Observatory
Nixon	Leif	EGI
Northcutt	Amy	NSF [attended Sep 30 only]
Oehlert	Sam	NCSA
Orlikowski	Victor	Duke University
Paxson	Vern	UC Berkeley / ICSI
Pearson	Doug	REN-ISAC / Indiana University
Petersen	Rodney	EDUCAUSE
Peterson	Greg	UT/NICS
Pulver	James	CLASSE Cornell University
Rackow	Gene	Argonne
Richmond	Ryan	AURA
Rieker	Thomas	NSF [attended Sep 30 only]
Rohler	Brian	NEEScomm/Purdue
Sakai	Scott	San Diego Supercomputer Center
Schipp	Jon	NCSA
Servilla	Mark	LTER Network
Sinatra	Michael	ESNet
Singer	Abe	LIGO
Slagell	Adam	University of Illinois
Smiley	Edward	The Pennsylvania State University
Sommer	Robin	ICSI/LBNL
Sorensen	Phillip	CLASSE (Cornell University)
Spencer	Kristin	NSF [attended Sep 30 only]
Sun	Werner	Cornell University
Thomas	Vic	BBN Technologies
Thompson	Kevin	NSF [attended Sep 30 only]
Towns	John	NCSA/XSEDE
Vieglais	Dave	DataONE
Wallace	Larry	Caltech
Welch	Von	CTSC/Indiana U.

Appendix B
Agenda

2013 NSF Cybersecurity Summit for Cyberinfrastructure and Large Facilities

Designing Cybersecurity Programs in Support of Science

September 30 - October 2, 2013

Hilton Arlington (near NSF) - Arlington, VA

- AGENDA -

Updated September 25th, 2013

Organizers: James Marsteller, Craig Jackson, Von Welch
jam@psc.edu, scjackso@indiana.edu, vwelch@indiana.edu

The theme for the 2013 NSF Cybersecurity summit is ***Designing Cybersecurity Programs in Support of Science***. This theme suggests a number of challenges to be addressed: How do we build a community for sharing experiences and supporting continuity between projects? What are the goals of a cybersecurity plan for the vast variety of NSF projects; what are the key motivations, assets and threats? How are we similar to and different from other communities addressing cybersecurity (e.g, higher education, government, private sector), and how do we relate to them?

The ideal summit attendee can speak to the needs of the science mission of their project or community has for cybersecurity, as well as the social, human resource, policy and other challenges for creating a cybersecurity program that leaves their community comfortable those needs have been met.

Day 1 (Sep 30): Optional parallel tutorials in the afternoon (1-5pm)

- Open to all attendees; registration required
- Registration Opens: 12pm
- Afternoon Coffee Break: 3:00pm - 3:30pm
- **Building a Cybersecurity Program (CTSC team)**
 - *Location: Da Vinci Room*
 - *Description:* This tutorial will provide principal investigators, project leaders, and project managers planning, building and operating scientific cyberinfrastructure with a method for accessing their security needs, documenting an action plan for addressing those needs, and quantifying resource requirements. Specifically, this tutorial will provide an overview and process for developing a cybersecurity plan for scientific computing projects. Discussion will focus on why security is crucial to an organization and things that senior management can do to establish a proactive stance on cybersecurity. This tutorial will present an overview of security issues that face NSF cyber infrastructure projects. The intent is to give PI's and managers an understanding of these issues and tools to address them.
- **Bro Network Intrusion Detection (Seth Hall, Sam Oehlert, Dr. Adam Slagell)**
 - *Location: Matisse Room*

- *Description:* Bro is a stateful, protocol aware open source high speed network monitor with applications as a next generation intrusion detection system, real time network discovery tool, historical network analysis tool, real time network intelligence, and dynamic active response. Originally developed by Vern Paxson, he now leads the core team of developers/researchers at both the International Computer Science Institute in Berkeley, CA and the National Center for Supercomputing Applications in Urbana-Champaign, IL. Bro provides a security team with logs of highly structured data about their network, a turing complete scripting language through which they can interact with real time stateful network events, and flexible open interfaces through which Bro can be programmed. Pragmatically able to interface with the entire network stack, Bro includes support for IPv6, tunneled traffic, SSL and more. In this presentation we present multiple case studies and are releasing their corresponding Bro scripts with source.
- *Please note* that a virtual box VM will be made available prior to this training session. To fully participate, attendees will get this running on their laptops ahead of time.
- **Secure Coding Practices (Prof. Barton Miller & Prof. Elisa Heymann)**
 - *Location:* Renoir Suite
 - *Description:* Security is crucial to the software that we develop and use. With the growth of both Grid and Cloud 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. 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 presents coding practices subject to vulnerabilities, with examples of how they commonly arise, techniques to prevent them, and exercises to reinforce them. Most examples are in Java, C, C++, Perl and Python, and come from real code belonging to Cloud and Grid systems we have assessed. This tutorial is an outgrowth of our experiences in performing vulnerability assessment of critical middleware, including Google Chrome, Wireshark, Condor, SDSC Storage Resource Broker, NCSA MyProxy, INFN VOMS Admin and Core, and many others.
- **Streamlining Collaboration with InCommon and Identity Federations (Warren G. Anderson and Dr. Jim Basney)**
 - *Location:* Picasso Room
 - *Description:* Because of the success of programs like XSEDE and OSG more and more scientists have access to more computing power than ever and consequently are generating more output than ever before. Efficiently sharing all those generated results with colleagues and collaborators, however, remains a problem--it's too difficult for scientists from different projects and different campuses to quickly and easily find spaces to collaborate. One of the largest barriers to efficient collaboration is creating and managing new electronic

identities for every new tool or web application. Federated identity can help and identity federations like InCommon in the US provide ready to consume identities that help streamline getting scientists into the same applications and spaces so they can collaborate. This tutorial will discuss what are federated identities, why we can trust them, and how to leverage a federation like InCommon and similar federations around the world to support discovery across VOs. We will focus on LIGO's experiences and lessons learned during their five year effort to build an end-to-end identity management infrastructure that consumes federated identity in support of collaboration with other astronomy and astrophysics projects.

Day 2 (Oct 1): Main plenary for all attendees in Gallery II/III (8am-5pm)

- 7:00 am: Registration and continental breakfast.
- 8:00 am: Welcome and Goals (Jim Marsteller)
- 8:20 am: Intro by NSF (Cliff Jacobs)
- 8:45 am: Opening Keynote - Vern Paxson
 - Focused on community building for cybersecurity
- 9:45 am: Coffee Break
- 10:00 am: Panel and discussion on community building - real world experiences from communities for cybersecurity and otherwise
 - Confirmed Panelists: Joel Cutcher-Gershenfeld, Jim Marsteller, Leif Nixon, Rodney Petersen
 - Moderator: Peter Arzberger
- 11:00 am: Panel and discussion on the goals of a cybersecurity program
 - Confirmed Panelists: Brian Bockelman, Cliff Jacobs, John Towns
 - Moderator: Ardoth Hassler
- 12:00 pm: Lunch (in Masters Ballroom)
- 1:00 pm: NSF remarks (Dr. Farnam Jahanian, CISE/NSF)
- 1:15 pm: A view from the field of NSF cybersecurity challenges, goals, and opportunities (Von Welch, CTSC PI)
- 1:45 pm: Panel and discussion on differences, similarities and relationships between NSF projects and other organizations (e.g., higher education, government, private sector)
 - Confirmed Panelists: Michael Bailey, Michael Corn, Vic Thomas
 - Moderator: Greg Bell
- 3:00 pm: Coffee Break
- 3:30 pm: Evolution of Network Security Threats and Capabilities for Science Communities (Adam Slagell)
- 4:00 pm: Open discussion - Recap progress towards goals. Refine topics to address in working groups on Day 3. (Jim Marsteller and Von Welch)
- 4:45 pm: Closing remarks. (Jim Marsteller, Cliff Jacobs)

- Present path forward on collaboration until next summit.
- 5:00 pm: Adjourn (dinner on own)

Day 3 (Oct 2): Break out into working groups for morning (8am-Noon)

- A long-term goal for the summit and CTSC is to build and support community that spans from year to year. Participants are invited to join one of the following four working groups. The primary goal for each group is to define a problem statement or charter around the working group topic to serve as a basis for collaboration after the 2013 summit, and feeding into the anticipated 2014 summit. Participants will have the opportunity to join dedicated groups in the Trusted CI Forum (trustedci.groupsite.com) to continue working together. In support of this goal, Day 3 objectives for each group may include (a) identifying the most critical and vexing questions for making progress in the topic area, (b) identifying resources and expertise that can be leveraged to address these challenges, and (c) identifying ways to usefully build community and communication around the topic area. Topics for the groups are:
 - a. Cybersecurity Planning & Programs Group (Jim Marsteller, moderator)
 - b. Identity & Access Management Group (Jim Basney, moderator)
 - c. Network Security & Monitoring Group (Adam Slagell, moderator)
 - d. Unconference Group: *Focus TBD!* (Von Welch, moderator)
- 7:00 am: Continental breakfast provided.
- 8:00 am: Kick-off working groups (moderators)
- 10:00 am: Coffee Break
- 10:30 am: Reconvene working groups
- 11:30 am: Recap discussion, post-summit steps (moderators)
- Noon: Adjourn (lunch on own)

Reference Materials

Past Summit Reports

- 2009: <http://net.educause.edu/ir/library/pdf/PUB1001.pdf>
- 2008: <http://net.educause.edu/ir/library/pdf/PUB9002.pdf>
- 2007: <http://www-cdn.educause.edu/ir/library/pdf/CYB0701.pdf>
 - NSF Response: <http://net.educause.edu/ir/library/pdf/CYB08006B.pdf>
- 2005: <http://net.educause.edu/ir/library/pdf/CYB0525.pdf>
 - NSF Response: <http://net.educause.edu/ir/library/pdf/CYB0525c.pdf>
- 2004: <http://net.educause.edu/ir/library/pdf/CSD4296.pdf>

Scientific Software Security Innovation Institute Workshops: <http://security.ncsa.illinois.edu/s3i2/>

"Cybersecurity 2011... and beyond. What Makes a Good Security Plan?" Ardoth Hassler, Senior IT Advisor, National Science Foundation. Associate VP University Information Services, Georgetown University: <http://trustedci.org/s/Cybersecurity-for-Managers-LF-Group-0106-2011.pptx>

NSF Cooperative Agreement Supplemental Financial & Administrative Terms and Conditions for Managers of Large Facilities. Effective February 1, 2012. Information Security Requirements (p. 6, item 56).

Appendix C
Bios for Speakers, Program Committee, and Organizers

2013 NSF Cybersecurity Summit for Cyberinfrastructure and Large Facilities

*

Bios for Speakers, Program Committee, and Organizers

in alphabetical order by surname

Warren Anderson is a gravitational wave physicist who has been part of the LIGO Scientific Collaboration since 1998. Along with his physics work, Warren has been active in LIGO computing, including working on the LIGO Computer Security Team and helping to found and grow the LIGO Identity and Access Management (LIAM) group. He is currently the project manager for the LIAM.

*

Dr. **Peter Arzberger** is Senior Science Advisor, Office of the Director (OD), National Science Foundation. Dr. Arzberger comes to NSF from the University of California, San Diego where he serves as the Founding Chair of the Pacific Rim Application and Grid Middleware Assembly (PRAGMA), an NSF-funded program developing collaborations, advancing application use and development of cloud and grid technologies, and student interactions throughout Pacific Rim institutions. He is also the Director of National Biomedical Computation Resource (NBCR), focusing on advanced computational technology to better enable biomedical research. His research has received wide ranging support from NSF, NIH, the Gordon and Betty Moore Foundation and the state of California, and has focused on broad interests in computational and data-driven biology, application-driven cloud and grid utilization and development, global sensor networks in ecology - in particular lake sciences via the Global Lake Ecological Observatory Network (GLEON), and models of international collaboration for researchers and students. He has also served as Director, Life Science Initiatives, UCSD; Executive Director, National Partnership for Advanced Computational Infrastructure (NPACI); and the Executive Director and Deputy Director, San Diego Supercomputer Center.

At NSF, Dr. Arzberger has served as a Program Director, 1988-1995, in the Divisions of Mathematical Sciences and Biological Infrastructure; as Division Director, Biological Infrastructure, 2009-2010; and as Acting Assistant Director and Senior Advisor, Directorate of Computer and Information Science and Engineering (CISE), 2010-2011. He served as a member of the NSF Advisory Committee for International Science and Engineering from 2012 to 2013.

Dr. Arzberger received his B.S. degree (1974) in mathematics from the University of Massachusetts; M.S. degree (1979) in statistics and Ph.D. (1983) in mathematics from Purdue University.

*

Michael Bailey is Associate Research Professor, LEO Adjunct Lecturer, and Co-Director of the Network and Security Research Group, University of Michigan. Professor Bailey's research is focused on the security and availability of complex distributed systems. His work informs both the development of such systems as well as the sciences of computer security, network architecture and design, network

protocols, and distributed systems. His work has been funded by the National Science Foundation, the Department of Homeland Security, the Department of Defense, the Beyster Foundation, and a number of commercial networking and security firms. Michael received his PhD in Computer Science and Engineering from Michigan in 2006 and joined the faculty as a Research Scientist in 2007. Prior to U-M, he was the Director of Engineering at network security company Arbor Networks. He is a Senior Member of the IEEE.

*

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, and he leads the Distributed Web Security for Science Gateways project (www.sciencegatewaysecurity.org), which provides standards compliant authorization and delegation software for science gateways. Jim is also the security technical lead for XSEDE (www.xsede.org) Software Development and Integration (SD&I). 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://pti.iu.edu/ci/ciss/final-report>). Jim is an active participant in the Globus Security Committee, The Americas Grid Policy Management Authority, the CIC Identity Management Taskforce, 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.

*

Greg Bell is Director of the Scientific Networking Division at Lawrence Berkeley National Laboratory (Berkeley Lab), and Director of the Energy Sciences Network (ESnet), the US Department of Energy's high-performance networking facility, engineered and optimized for large-scale science. Bell joined ESnet in 2010. Previously, he worked in Berkeley Lab's IT Division as Chief Technology Architect, reporting to the CIO. Bell's professional interests include advanced networking, security models for open science, collaborative tools, sustainable IT, cloud services, and high-performance computing.

*

Dr. **Rakesh B. Bobba** is a Research Assistant Professor in the College of Engineering at the University of Illinois, Urbana-Champaign with appointments in Information Trust Institute and Electrical and Computer Engineering Department. His research interests are in the security of distributed and networked systems with a current focus on cyber-physical systems including critical infrastructures such as the power grid and cloud computing. He received M.S. and Ph.D. degrees in Electrical and Computer Engineering from the University of Maryland at College Park in 2007 and 2009, respectively.

*

Brian Bockelman leads the Open Science Grid Technology area, which is charged with planning and executing the technology evolution of the OSG. The OSG maintains a production grid infrastructure. Its

software stack (containing middleware such as HTCondor, Globus, and Xrootd) is deployed at over 100 sites, primarily academic clusters and labs. In the last few years, the OSG has been evolving its trust model to become more "user friendly" without sacrificing security. Brian's other roles include PI on the Lark project, for integrating the network and high-throughput computing layers and technical lead on the "Any Data, Any Time, Anywhere" project for improving data accessibility in High Energy Physics. Brian is a faculty member of the Computer Science and Engineering department at the University of Nebraska-Lincoln.

*

Scott Campbell began working at LBNL/NERSC in April of 2002 on network security. Scott works on the Bro intrusion detection systems and incident response. Prior to LBNL, Scott has worked extensively in industry in the areas of Unix and network administration. Scott holds a bachelor of science degree in Physics from San Francisco State University.

*

Michael Corn is the senior Security and Privacy Officer for the Urbana campus as well as the Chief Information Security Officer for the University of Illinois. In addition to overseeing the campus Security and Privacy Office, his recent and ongoing responsibilities include CALEA, PCI, security and privacy provisions in contracts for electronic services, strategic procurement, and information policy for the campus. Michael is a member of the Educause CALEA Technical Team and the State of Illinois PKI Policy Board. He is a graduate of the University of Colorado at Boulder and the University of Illinois at Urbana-Champaign. He has prior experience on the NSF Cybersecurity Summit Program Committee.

*

Joel Cutcher-Gershenfeld is a Professor and former Dean in the School of Labor and Employment Relations (LER) at the University of Illinois. He is also a Senior Research Scientist with the National Center for Super Computing Applications (NCSA) and holds a courtesy appointment in Industrial and Enterprise Systems Engineering (IESE) at the University of Illinois. Joel also serves as a visiting Professor in Work and Organizations at the University of Sydney, Australia.

He is an award-winning author who has co-authored or co-edited ten books, including *Multinational Human Resource Management and the Law* (Edward Elgar, forthcoming), *Valuable Disconnects in Organizational Learning Systems* (Oxford University Press, 2005), *Lean Enterprise Value* (Palgrave, 2002), *Knowledge-Driven Work* (Oxford University Press, 1998), and *Strategic Negotiations* (Harvard Business School Press, 1994), and over eighty five articles on high performance work systems, transformation in labor-management relations, negotiations and conflict resolution, economic development, and engineering systems. His current research centers on stakeholder alignment in complex systems – a foundation for 21st Century institutions. Along with his co-inventors, he has a patent pending on a new visualization method designed to help see points of alignment and misalignment among stakeholders.

Joel was the 2009 President of the Labor and Employment Relations Association (LERA). Prior to coming

to the University of Illinois, Joel served as a Senior Research Scientist and Executive Director of the Engineering Systems Learning Center, with a joint appointment in MIT's Sloan School of Management and MIT's Engineering Systems Division, as well as a Visiting Associate Professor at Babson College, and an Associate Professor at Michigan State University.

Joel has extensive experience leading large-scale systems change initiatives with public and private stakeholders in Australia, Bermuda, Canada, Denmark, England, Iceland, Italy, Jamaica, Mexico, New Zealand, Panama, Poland, Spain, South Africa, and the United States. He holds a Ph.D. in Industrial Relations from MIT and a B.S. in Industrial and Labor Relations from Cornell University.

*

Patrick Duda is a member of NCSA's Cybersecurity directorate and is currently assigned to work on CTSC. His responsibilities are to aid in the EOT efforts under the direction of Randy Butler. Most of this work is aimed at developing training programs to disseminate security information to NSF funded CI projects. Prior to joining NCSA Patrick worked with several software development companies. At NCSA he has worked on GRID computing and various other science projects.

*

Deborah A. Frincke is Deputy Director for Research at the National Security Agency. Dr. Frincke's research spans a broad cross section of computer security with a focus on infrastructure defense and computer security education. Before joining NSA, she was Chief Scientist for Cyber Security at Pacific Northwest National Laboratory (PNNL). At PNNL since 2004, Dr. Frincke led their internal research investment in cyber security. Additionally, she is an Affiliate Professor at the University of Washington's Information School. Prior to her tenure at PNNL, Dr. Frincke was a full professor at the University of Idaho and co-founder/co-director of their Center for Secure and Dependable Systems, one of the first such institutions to receive NSA's designation of a National Center of Excellence in Information Assurance Education. Moreover, she was one of the four original co-founders of TriGeo Network Security, where she served as Lead Scientist and CTO. Dr. Frincke earned her bachelor's degree in computer science and mathematics from the University of California, Davis, and her master's and doctorate degrees in computer science from University of California, Davis.

*

After receiving a bachelor's degree in Geography from the Ohio State University **Seth Hall** began full time work in the OSU Network Security team where he began working with Bro. Later he headed to General Electric to work on deploying Bro more broadly within that organization. Shortly afterward he started with the International Computer Science Institute under an NSF grant to solidify and expand Bro. He's currently still at ICSI, but also taking on commercial work with Bro as a co-founder of Broala.

*

Ardoth Hassler is Associate Vice President of University Information Services & Executive Director, Office of Assessment and Decision Support at Georgetown University. There, her work focuses on

analytics, institutional research, business intelligence, data warehousing and reporting as well as planning, policy and research. She 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, as well as other important projects. In 2009 and 2010, she received Director's Awards for her work with the Got Green team. She has prior experience on the NSF Cybersecurity Summit Program Committee. She has a BS in Math (CS minor) from Oklahoma State University and an MS in Biostatistics from the University of Oklahoma.

*

Randy Heiland is a Senior Systems Analyst and Programmer at Indiana University's Center for Applied Cybersecurity Research. He is a computer scientist (M.S., U. Utah '85) and applied mathematician (M.A., Arizona State U. '92) who has worked in industry, government labs, and academia. In 2003, he joined IU's Pervasive Technology Labs (now the Pervasive Technology Institute) as an Associate Director of the Scientific Data Analysis Lab at IUPUI. While at IU, he has contributed to projects at the Medical School, UITS Research Technologies, and grant-funded (NSF and NIH) software development projects that included Purdue's Dept. of Chemistry, IU's Dept. of Physics, and IU's School of Informatics and Computing. He is currently contributing to the NSF-funded [Center for Trustworthy Scientific Cyberinfrastructure](#).

*

Prof. **Elisa Heymann** received her B.S. in Computer Science from Universidad Simon Bolvar (Venezuela) in 1992. She also received the M.S. and Ph.D. degrees in Computer Science from the Universitat Autònoma de Barcelona (Spain) in 1995 and 2001 respectively. She is an Associate Professor in the Computer Architecture and Operating Systems Department. She co-directs the MIST software vulnerability assessment project in collaboration with her colleagues at the University of Wisconsin Madison. She is also in charge of the Grid group at the UAB, and currently she participates in two major Grid European Projects: EGI-InSPIRE and European Middleware Initiative (EMI). Heymann co-chaired the Shonan Seminar on Grid and Cloud Security (October 2012). Her research interests include security and resource management for Grid and Cloud environments. This research is supported by the Spanish government, the European Commission, and NATO.

*

Craig Jackson is a policy analyst and project manager at Indiana University's Center for Applied Cybersecurity Research. He is a graduate of the IU Maurer School of Law (JD '10) and IU School of Education (MS '04). His project management, research, and design 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. As a member of the Indiana bar, he has litigated state and federal court. His interests include cybersecurity, privacy, identity management, and criminal justice policy and law, as well

as risk management and theory.

*

Dr. **Cliff Jacobs** has been at the National Science Foundation (NSF) for 28 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). Currently, he is an expert with the Division Advanced Cyberinfrastructure. Dr. Jacobs has represented the geosciences in a variety of NSF studies and initiatives related to high performance computing and information technology, observing facilities, and best practices in the operation and management of facilities. As chair of the internal working group on cybersecurity for NSF large facilities, Dr. Jacobs supported the development of five community workshops and helped to craft cybersecurity language in the cooperative agreements for large facilities.

Dr. Jacobs received his Bachelor of Arts degree in Mathematics from Texas A&M University and his Master of Science degree in Oceanography, also from Texas A&M University. His Doctor of Philosophy degree was awarded by New York University in Oceanography.

*

Dr. **Farnam Jahanian** serves as the National Science Foundation Assistant Director for the Computer and Information Science and Engineering (CISE) Directorate. He guides CISE in its mission to uphold the nation's leadership in scientific discovery and engineering innovation through its support of fundamental research in computer and information science and engineering and transformative advances in cyberinfrastructure. Dr. Jahanian oversees the CISE budget of over \$850 million, directing programs and initiatives that support ambitious long-term research and innovation, foster broad interdisciplinary collaborations, and contribute to the development of a computing and information technology workforce with skills essential to success in the increasingly competitive, global market. He also serves as co-chair of the Networking and Information Technology Research and Development (NITRD) Subcommittee of the National Science and Technology Council Committee on Technology, providing overall coordination for the activities of 14 government agencies.

Dr. Jahanian holds the Edward S. Davidson Collegiate Professorship in Electrical Engineering and Computer Science at the University of Michigan, where he served as Department Chair for Computer Science and Engineering from 2007 - 2011 and as Director of the Software Systems Laboratory from 1997 - 2000. Earlier in his career, he held research and management positions at the IBM T.J. Watson Research Center.

Over the last two decades at the University of Michigan, Dr. Jahanian led several large-scale research projects that studied the growth and scalability of the Internet infrastructure, which ultimately transformed how cyber threats are addressed by Internet Service Providers. His research on Internet infrastructure security formed the basis for the successful Internet security services company Arbor Networks, which he co-founded in 2001. Dr. Jahanian served as Chairman of Arbor Networks until its acquisition in 2010.

Dr. Jahanian is the author of over 100 published research papers and has served on dozens of national advisory boards and panels. His work on Internet routing stability and convergence has been highly influential within both the network research and the Internet operational communities and was recognized with an ACM SIGCOMM Test of Time Award in 2008. He has received numerous other awards for his innovative research, commitment to education, and technology commercialization activities. He was named Distinguished University Innovator at the University of Michigan (2009) and received the Governor's University Award for Commercialization Excellence (2005).

Dr. Jahanian holds a master's degree and a Ph.D. in Computer Science from the University of Texas at Austin. He is a Fellow of the Association for Computing Machinery (ACM), the Institute of Electrical and Electronic Engineers (IEEE), and the American Association for the Advancement of Science (AAAS).

*

As the Information Security Officer of the Pittsburgh Supercomputing Center, **James A. Marsteller, Jr.** (CISSP) is responsible for ensuring the availability and integrity of the PSC's high performance computing assets. Jim has over 12 years experience in the information security field and greater than 17 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 two most recent past summits, in 2008 and 2009.

*

Dr. **Michael McLennan** is a senior research scientist in research computing at Purdue University, where he is Director of the HUBzero® Platform for Scientific Collaboration. HUBzero powers nanoHUB.org, NEES.org, and more than 50 other Web sites supporting both education and research. All together, these sites served more than 1,000,000 visitors worldwide during the past 12 months alone.

Dr. McLennan received a Ph.D. in 1990 for his dissertation on dissipative quantum mechanical electron transport in semiconductor heterostructure devices. He spent 14 years working in industry at Bell Labs and Cadence Design Systems, developing software for computer-aided design of integrated circuits. He created [incr Tcl], an object-oriented extension of the Tcl scripting language, which has been used by thousands of developers worldwide on projects ranging from the TiVo digital video recorder to the Mars Pathfinder.

*

Prof. **Barton Miller** is a professor of computer science at the University of Wisconsin Madison. Prof. Miller founded the field of fuzz random testing, which is foundational to computer security and software testing. In addition, he founded (with his then-student Prof. Jeffrey Hollingsworth) the field of dynamic binary instrumentation, which is a widely used, critical technology for cyberforensics. Prof. Miller advises the Department of Defense on computer security issues through his position at the Institute for Defense Analysis and was on the Los Alamos National Laboratory Computing, Communications and Networking

Division Review Committee and the US Secret Service Electronic Crimes Task Force (Chicago Area). He is currently an advisor to the Wisconsin Security Research Council. Prof. Miller is a fellow of the ACM.

*

Leif Nixon is based at the National Supercomputer Centre (NSC), Linköping University, Sweden. He has 15 years of experience in IT security, mainly in an operational role. In addition to serving as Security Officer for the Nordic e-Infrastructure Collaboration and the Swedish national grid infrastructure, he also heads the incident response task force for the European Grid Infrastructure (EGI).

*

Sam Oehlert is a security engineer at NCSA. Day to day, Sam works in operational security. His duties includes incident response, system administration for the security group, and security projects including acting as the lead bro user in the group. He graduated from the University of Illinois in Urbana-Champaign in 2010 and has been working at NCSA since graduating.

*

Vern Paxson is a professor of Electrical Engineering and Computer Sciences at UC Berkeley and leader of the Networking and Security group at the International Computer Science Institute in Berkeley. His research focuses heavily on measurement-based analysis of network activity and Internet attacks. He has worked extensively on high performance network monitoring and on cybercrime, and co-directs the Center for Evidence-based Security Research (www.evidencebasedsecurity.org).

*

Rodney Petersen is Managing Director of the EDUCAUSE Washington Office. He also directs the EDUCAUSE Cybersecurity Initiative and is the lead staff liaison for the Higher Education Information Security Council. Prior to joining EDUCAUSE, he served as the Director of IT Policy and Planning in the Office of the Vice President and Chief Information Officer at the University of Maryland. He is the co-editor of a book in the EDUCAUSE Leadership Strategy Series entitled "Computer and Network Security in Higher Education". He received his law degree from Wake Forest University. He also received a certificate as an Advanced Graduate Specialist in Education Policy and Leadership from the University of Maryland.

*

Mark Servilla is Lead Scientist, Network Information System at LTER Network Office (LNO). At LNO, Mr. Servilla's primary responsibility is the implementation of the LTER Network Information System—a system of standards and applications that support the interoperability of distributed LTER research sites, thus enabling synthetic science at the Network level and beyond. To achieve a successful Network Information System, he will rely on his skills as a computer scientist to use the latest computing technologies for maximum effectiveness within the NIS, while utilizing his experience as an earth scientist to better serve the needs and understand the requirements of LTER, associated scientists, and the field

of Ecology in general. Prior to his current position at LNO, Mark's most recent role in the private sector at Photon Research Associates (PRA), Inc. was as architect of a web-based application (GeoServer TM) that provided the discovery, management, and exploitation of geospatial data, including Earth observation imagery and GIS vector objects. Mark holds graduate degrees in Earth and Planetary Sciences (Volcanology) and Computer Science, both from the University of New Mexico.

*

Adam Slagell is a senior research scientist in the Cyber Security Directorate at the NCSA, the Chief Information Security Officer, a member of the University Information Security Committee, and the leader of several projects that blend research and development activities. His most notable current activities are as leader of the Bro development efforts at NCSA and the Blue Waters Petascale computing system's security architect.

Adam completed his Masters in mathematics at Northern Illinois University and his Masters in computer science at the University of Illinois Urbana-Champaign where he was focused on number theory and applied cryptography. After graduation he joined the NCSA where he has been working in the security group for the past 10 years.

*

Robin Sommer is a Senior Researcher at the International Computer Science Institute, Berkeley, and he is also a member of the cyber-security team at the Lawrence Berkeley National Laboratory. Robin Sommer's research focuses on network security and privacy, with a particular emphasis on high-performance network monitoring in operational settings. He is leading the development of the open-source Bro network security monitor, and he is a co-founder of Broala, a recent start-up offering professional Bro services to corporations and government.

*

Dr. **Vicraj (Vic) Thomas** is a Scientific Director at BBN Technologies. He leads the Experimenter Support and Advocacy group within the GENI Project Office. The GENI Project Office provides the NSF with program management and systems engineering support in the design and development of GENI. GENI is a suite of research infrastructure rapidly taking shape across the United States. It is well suited for exploring networks at scale, thereby promoting innovations in network science, security, services and applications.

Dr. Thomas' research interests include dependable systems and systems security. In the past he was a co-PI on an intrusion detector correlation project funded by the DARPA CyberPanel program and the PI of a project on the DARPA Cougaar program that developed intrusion detection agents. On the GENI project, Dr. Thomas was one of the systems engineers that developed a security plan for GENI.

*

John Towns is Director of the Collaborative eScience Programs Office at the National Center for

Supercomputing Applications (NCSA) at the University of Illinois. He is also PI and Project Director for the Extreme Science and Engineering Discovery Environment (XSEDE) project and the Operations Manager for the Illinois Campus Cluster Program. Towns plays significant roles in the deployment and operation of high-end resources and services, and distributed computing projects. His background is in computational astrophysics utilizing a variety of computational architectures with a focus on application performance analysis. At NCSA, he provides leadership and direction in the support of an array of computational science and engineering research projects making use of advanced computing resources and services. He earned M.S. degrees in Physics and Astronomy from the University of Illinois and a B.S. in Physics from the University of Missouri-Rolla.

*

Von Welch is the deputy director of Indiana University's Center for Applied Cybersecurity Research (CACR) and PI for the Center for Trustworthy Scientific Cyberinfrastructure, a project dedicated to helping NSF science projects with their cybersecurity needs. 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 the Open Science Grid as an identity management expert. 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.

Appendix D
Handout

2013 NSF Cybersecurity Summit for Cyberinfrastructure and Large Facilities

Designing Cybersecurity Programs in Support of Science

September 30 - October 2, 2013

Hilton Arlington (near NSF) - Arlington, VA

Organizers: James Marsteller, Craig Jackson, Von Welch

<http://trustedci.org/2013-nsf-cybersecurity-summit>

The theme for the 2013 NSF Cybersecurity summit is Designing Cybersecurity Programs in Support of Science. This theme suggests a number of challenges to be addressed: How do we build a community for sharing experiences and supporting continuity between projects? What are the goals of a cybersecurity plan for the vast variety of NSF projects; what are the key motivations, assets and threats? How are we similar to and different from other communities addressing cybersecurity (e.g., higher education, government, private sector), and how do we relate to them?

MONDAY, SEPTEMBER 30

Registration Opens: 12:00pm

Optional parallel tutorials in the afternoon: 1:00pm - 5:00pm

Afternoon Coffee Break: 3:00pm - 3:30pm

Building a Cybersecurity Program (CTSC team)

Location: Da Vinci Room

Bro Network Intrusion Detection (Seth Hall, Sam Oehlert, Dr. Adam Slagell)

Location: Matisse Room

Secure Coding Practices (Prof. Barton Miller & Prof. Elisa Heymann)

Location: Renoir Suite

Streamlining Collaboration with InCommon and Identity Federations

(Warren G. Anderson and Dr. Jim Basney)

Location: Picasso Room

SSID
attwifi

Access Code
BANQUET (case-sensitive)

**Please connect with
only one device at a time
to contain both cost and
bandwidth*

WIFI

Join the Trusted CI Forum
for online discussion during
the summit:

[https://trustedci.
groupsie.com/join](https://trustedci.groupsie.com/join)

CONNECT

THIS EVENT SUPPORTED BY:



This event is supported in part by the National Science Foundation under Grant Number OCI-1234408. Any opinions, findings, and conclusions or recommendations expressed are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

TUESDAY, OCTOBER 1

Main plenary for all attendees in Gallery II/III (8 am-5 pm)

7:00 am: **Registration and Continental Breakfast**

8:00 am: **Welcome and Goals** (Jim Marsteller)

8:20 am: **Intro by NSF** (Cliff Jacobs)

8:45 am: **Opening Keynote** (Vern Paxson, ICSI)
Focused on community building for cybersecurity

9:45 am: **Coffee Break**

10:00 am: **Panel and Discussion on Community Building - Real World Experiences from Communities for Cybersecurity and Otherwise**

Joel Cutcher-Gershenfeld, Jim Marsteller, Leif Nixon, Rodney Petersen

Moderator: Peter Arzberger

11:00 am: **Panel and Discussion on the Goals of a Cybersecurity Program**

Brian Bockelman, Cliff Jacobs, John Towns

Moderator: Ardoth Hassler

12:00 pm: **Lunch** (in Masters Ballroom)

1:00 pm: **NSF Remarks** (Dr. Farnam Jahanian, CISE/NSF)

1:15 pm: **A View from the Field of NSF Cybersecurity Challenges, Goals, and Opportunities**
(Von Welch, CTSC PI)

1:45 pm: **Panel and Discussion on Differences, Similarities and Relationships Between NSF Projects and Other Organizations (e.g., Higher Education, Government, Private Sector)**

Michael Bailey, Michael Corn, Vic Thomas

Moderator: Greg Bell

3:00 pm: **Coffee Break**

3:30 pm: **Evolution of Network Security Threats and Capabilities for Science Communities**
(Adam Slagell, NCSA)

4:00 pm: **Open Discussion** - Recap progress toward goals. Refine topics to address in working groups on Day 3.
(Jim Marsteller and Von Welch)

4:45 pm: **Closing Remarks** (Jim Marsteller, Cliff Jacobs)
Present path forward on collaboration until next summit

WEDNESDAY, OCTOBER 2

7:00 am: **Continental Breakfast**

8:00 am: **Kick-off Working Groups** (moderators)

Break out into working groups for morning (8am-Noon)

Topics for the groups are:

- *Cybersecurity Planning & Programs Group* (Jim Marsteller, moderator)
- *Identity & Access Management Group* (Jim Basney, moderator)
- *Network Security & Monitoring Group* (Adam Slagell, moderator)
- *Unconference Group: Focus TBD!* (Von Welch, moderator)

10:00 am: **Coffee Break**

10:30 am: **Reconvene Working Groups**

11:30 am: **Recap Discussion, Post-summit Steps** (moderators)

12:00 pm: **Adjourn** (lunch on own)

SPEAKER BIOGRAPHIES
are available online at:

www.trustedci.org/2013-nsf-cybersecurity-summit

WEDNESDAY, OCTOBER 2

special thanks to:

THE PROGRAM COMMITTEE

Michael Bailey
Scott Campbell
Michael Corn
Deborah A. Frincke
Ardoth Hassler
Craig Jackson
James A. Marsteller
Rodney J. Petersen
Mark Servilla
Von Welch

NSF OBSERVERS

Cliff Jacobs
Kevin Thompson

Your feedback is very important to us:
<http://www.surveymonkey.com/s/2013NSFsummit>

Appendix E
Contingency Agenda for Day 2

NSF Cybersecurity for CI and Large Facility Contingency Agenda for Government Shutdown






Day 2 (Oct 1): Main plenary for all attendees in Gallery II/III (8am-5pm)

- 7:00 am: Registration and continental breakfast.
- 8:00 am: Welcome and Goals (Jim Marsteller)
- 8:20 am: Opening Keynote - Vern Paxson
 - Focused on community building for cybersecurity
- 9:20 am: Coffee Break (25 minutes early)
- 9:45 am: Panel and discussion on community building - real world experiences from communities for cybersecurity and otherwise
 - Confirmed Panelists: Michael McLennan, Jim Marsteller, Leif Nixon, Rodney Petersen
 - Moderator: Craig Jackson
- 11:00 am: Panel and discussion on the goals of a cybersecurity program
 - Confirmed Panelists: Brian Bockelman, John Towns, Ardoth Hassler
 - Moderator: Von Welch
- 12:00 pm: Lunch (in Masters Ballroom)
- 1:00 pm: A view from the field of NSF cybersecurity challenges, goals, and opportunities (Von Welch, CTSC PI)
- 1:35 pm: Panel and discussion on differences, similarities and relationships between NSF projects and other organizations (e.g., higher education, government, private sector)
 - Confirmed Panelists: Michael Bailey, Michael Corn, Vic Thomas
 - Moderator: Greg Bell
- 3:00 pm: Coffee Break
- 3:30 pm: Evolution of Network Security Threats and Capabilities for Science Communities (Adam Slagell)
- 4:00 pm: Open discussion - Recap progress towards goals. Refine topics to address in working groups on Day 3. (Jim Marsteller and Von Welch)
- 4:45 pm: Closing remarks. (Jim Marsteller, Von Welch, Craig Jackson)
 - Present path forward on collaboration until next summit.
- 5:00 pm: Adjourn (dinner on own)

Appendix F
Attendee Survey Summary Report

Attendee Survey | 2013 NSF Cybersecurity Summit SurveyMonkey for Cyberinfrastructure and Large Facilities

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



		Response Percent	Response Count
Member / leader of an NSF project		61.0%	25
NSF Program Officer		0.0%	0
Campus IT Professional / CIO		31.7%	13
Cybersecurity Researcher		17.1%	7
Personnel from another federal program (NSA, DOE/ESNet, etc.)		4.9%	2
Other		7.3%	3

If applicable, please state your NSF Project and/or affiliated NSF Directorate. Other comments or clarifications are welcome. 22

answered question **41**

skipped question **0**




2. Where do you work primarily?

		Response Percent	Response Count
State/Province:		92.3%	36
Country:		100.0%	39


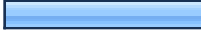

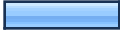

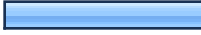
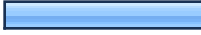


answered question **39**

skipped question **2**




3. How would you rate your level of familiarity with cybersecurity?

		Response Percent	Response Count
Novice		10.0%	4
Intermediate		45.0%	18
Expert		45.0%	18
answered question			40
skipped question			1

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

		Response Percent	Response Count
Day 1: Building a Cybersecurity Program (CTSC team)		22.0%	9
Day 1: Bro Network Intrusion Detection (Seth Hall, Sam Oehlert, Dr. Adam Slagell)		29.3%	12
Day 1: Secure Coding Practices (Prof. Barton Miller & Prof. Elisa Heymann)		14.6%	6
Day 1: Streamlining Collaboration with InCommon and Identity Federations (Warren G. Anderson and Dr. Jim Basney)		17.1%	7
Day 2: Plenary Session		90.2%	37
Day 3: Cybersecurity Programs Group		29.3%	12
Day 3: Identity & Access Management Group		29.3%	12
Day 3: Network Security Group		26.8%	11
Day 3: Unconference Group		2.4%	1
		answered question	41
		skipped question	0

5. How would you rate your overall experience with the 2013 summit?

		Response Percent	Response Count
Excellent		39.0%	16
Good		56.1%	23
Average		4.9%	2
Below Average		0.0%	0
Poor		0.0%	0
answered question			41
skipped question			0

6. Please rate your experience with the 2013 summit in these areas:

	Excellent	Good	Average	Below Average	Poor	Rating Count
Topics Addressed	36.6% (15)	56.1% (23)	7.3% (3)	0.0% (0)	0.0% (0)	41
Quality of Presentations	39.0% (16)	53.7% (22)	7.3% (3)	0.0% (0)	0.0% (0)	41
Logistics & Organization	73.2% (30)	24.4% (10)	2.4% (1)	0.0% (0)	0.0% (0)	41
Venue	46.3% (19)	48.8% (20)	4.9% (2)	0.0% (0)	0.0% (0)	41
answered question						41
skipped question						0




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

		Response Percent	Response Count
A great deal better		2.4%	1
Quite a bit better		36.6%	15
Somewhat better		19.5%	8
About what was expected		34.1%	14
Somewhat worse		7.3%	3
Quite a bit worse		0.0%	0
A great deal worse		0.0%	0
answered question			41
skipped question			0



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

		Response Percent	Response Count
Extremely useful		9.8%	4
Very useful		53.7%	22
Moderately useful		31.7%	13
Slightly useful		4.9%	2
Not at all useful		0.0%	0
answered question			41
skipped question			0

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

		Response Percent	Response Count
Much too little time for informal networking		0.0%	0
Too little time for informal networking		9.8%	4
About the right balance		85.4%	35
Too little time for structured presentations		4.9%	2
Much too little time for structured presentations		0.0%	0
answered question			41
skipped question			0

10. Would you like to attend future summits?

		Response Percent	Response Count
Yes		85.4%	35
Maybe		14.6%	6
No		0.0%	0
answered question			41
skipped question			0

11. How can we improve the summit experience in the future?

	Response Count
	24
answered question	24
skipped question	17

12. Were there any aspects of the summit you found particularly useful or important? If so, please explain.

	Response Count
	23
answered question	23
skipped question	18

Pages 8 through 16 contain identifying, demographic information regarding specific respondents, and are not included in this report.

Q11. How can we improve the summit experience in the future?

1	Make the panel discussions more structured. Allow for more audience participation. Prod the participants more to participate on post-meeting discussions and sharing of documents.	Oct 26, 2013 12:58 PM
2	More insight/participation from NSF (not just because of Gov. shutdown: delegating cyber-security plan responsibility to awardee without a framework guarantees mis-alignment and friction for collaborations and continuity of access. More (any) minorities participation/insight (1 female!) everyone else was middle age and white (slight exaggeration, but it was the usual suspects from 10 years ago). Need the next generation, industry and more international insight. Also MUST to happen every year (NOT at year end!!!) and have coherent report-out/participation in other key events (XSEDE, SC, SANS etc)	Oct 11, 2013 5:34 AM
3	Increase the amount(time) and/or number of "hands-on" or interactive sessions.	Oct 8, 2013 2:42 PM
4	Pick a different government to work with :)	Oct 7, 2013 7:27 PM
5	My job is primarily in research operations, control systems, and data acquisition computing. I don't deal much in infrastructure or external network security, but need to be concerned about system level security and privileges and local networking among devices. I would have liked to see more about system level security.	Oct 7, 2013 10:00 AM
6	More technical hands-on workshops, or opportunity to attend more than one	Oct 7, 2013 8:35 AM
7	As mentioned in the third day, there was a noticeable lack of diversity in the audience representation. Gender and racial diversity are something that needs to be addressed, but in addition a less obvious thing that I noticed was a homogeneity in the way that we as a group seemed to look at and think about issues and problems. We as a group tend to be a bit older and subject to groupthink driven by historical bias. Perhaps getting some fresh ideas would help us?	Oct 7, 2013 6:58 AM
8	I think it'll be interesting to hear from a few users of our cyberinfrastructures: Do they think our cybersecurity mechanisms are getting in the way of their science? Do they think they are getting the security they need and how do they know if they are getting/not getting the security they need? What support, if any, can we give these users, esp. if they have users of their own. For example, can we provide them with some sort of privacy/security assurances that will help them get IRB approvals if their experiments need them?	Oct 7, 2013 6:39 AM
9	For the secure coding practices workshop, provide optional hands-on or, at least, a more thorough walk-through of secure coding vulnerabilities.	Oct 7, 2013 5:57 AM
10	There were 1 or 2 quite obnoxious people in the audience that dominated conversation (if you can call it that) even to the point of interrupting the keynote speaker. I'm not sure what can be done, but that was really the only negative beyond the government shutdown, which was completely outside of your control.	Oct 7, 2013 5:44 AM
11	Perhaps a clearer separation between a technical and a managerial track?	Oct 7, 2013 5:42 AM
12	More technical sessions on a variety of topics. For example: IDS systems, securing Linux/Windows, secure networking, system monitoring, honeypots,	Oct 4, 2013 5:12 AM

Q11. How can we improve the summit experience in the future?

success stories with commercial products, etc... More moderation of the discussions would have also been useful. Many were dominated by one or two people.

- | | | |
|----|--|----------------------|
| 13 | Perhaps fewer panels would be good. | Oct 3, 2013 10:13 AM |
| 14 | A few suggestions: 1) The summit was heavily skewed toward very large site and facilities. To some extent, this is already a well-established community; if the goal of the conference is to build up the NSF cybersecurity community, try inviting more people from outside of the community! The conference mostly had the "top 10" research computing sites; try to think how to include more representation of the "next 100". I would suggest looking at the list of CC-NIE awardees - these have a number of institutions aggressively investing in CI who, by definition, needed NSF assistance to accomplish their goals (and are thus probably on the smaller side). I think "the next 100" is a possible area of growth for the cybersecurity community. 2) The plenary session was "too large" in that folks could hide quietly in the back and check email. For future summits, consider not allowing laptops to be used in the conference hall or decrease the number of participants. 3) Unfortunately, the mix of plenary presentations skewed heavily toward network security. Try to include a mix from other aspects of cybersecurity. 4) There was an interesting dichotomy of policy and technology people on the invite list. I'm not sure if this is good or bad -- the two groups' interactions seemed to self-organize around their topics of interest. In terms of keep the focus of the summit, you may want to purposely lean one way or the other in the future. | Oct 3, 2013 7:35 AM |
| 15 | Overall, I think it went very well. It seems that we are forming working groups which we expect to work actively over the year. I think this is good, otherwise this is all just talk. So perhaps next year the 3rd day sessions are a combination of working group face to face meetings and breakout "form the next working groups" meetings. The only real problem is that all the topics were interesting, so choosing was hard. | Oct 3, 2013 6:46 AM |
| 16 | This summit seemed unfocused. While the title indicated large facilities, much of the time was spent discussing the tiny stuff. While they are important and need the most help, it's not what was expected. In many ways the audience was wrong for the small stuff discussions. There were some people there from small sites, but they rarely spoke up. Their perspectives were needed and in many ways surprising or unknown. Large facilities come with a larger staff and budget so scale and reuse is easier. For the little sites things need to be created and they don't have the staff or overhead money to accomplish it. There also needs to be some sort of icebreaker process early to get people to know who's in the room and make a connection. While many people there knew each other, for the newer or shy, they didn't know who to turn to with questions or common issues/problems. | Oct 3, 2013 5:25 AM |
| 17 | More concrete topics, more training opportunities. Better plenary presentations. | Oct 3, 2013 4:26 AM |
| 18 | Warren anderson did a great job covering LIGO, but 160 slides over 4 hours in one talk is just too much. Cut it to 2 hours max as a keynote case study, then get 4-6 other case studies together to do 30-45 minute talks. Bring them back on day 3 for a 60 minute panel. Attendee lists should be easier to find. Maybe get a QR code to the page that has the info. | Oct 2, 2013 6:16 PM |

Q11. How can we improve the summit experience in the future?

19	less general session, more targeting of specific areas, workshops, tools, and planning. Invite contributions in each. Work to build a community by identifying who is in it, what are there needs, and what are the common goals. Members should want to come again because the summit pays back the time and effort involved through training, resource sharing, and knowledge transfer.	Oct 2, 2013 10:26 AM
20	Consolidate half-day activities to single day (due travel constraints) or hold summit in more central location relative to USA.	Oct 2, 2013 10:26 AM
21	The hotel rates where funny. It was \$90 cheaper to come early and leave later. So I met with colleagues before and after we saved our project a considerable amount. I did book with the conference group code.	Oct 2, 2013 7:11 AM
22	Better moderated discussion. A few individuals tended to dominate the discussion.	Oct 2, 2013 6:53 AM
23	More time for the tech session.	Oct 2, 2013 6:51 AM
24	Maybe a less expensive hotel. Longer, more in-depth workshops; what you had this year was very useful but we ran out of time.	Oct 2, 2013 6:40 AM

Q12. Were there any aspects of the summit you found particularly useful or important? If so, please explain.

1	Learning of the cybersecurity challenges and best practices from all the other participants.	Oct 26, 2013 12:58 PM
2	Networking	Oct 11, 2013 10:25 AM
3	The willingness to move up the stack from network security. The awareness that openness is essential in research, but that accountability can't be delegated. Meeting organizers allowed free discussion, but kept the session topic in sight and maintained equal access. Great job!	Oct 11, 2013 5:34 AM
4	The small group sessions the third day. They provided insight on how other organizations operate, which generated good discussion, and ideas to take home.	Oct 8, 2013 2:42 PM
5	Both the Bro workshop and Identity Management group meetings were useful, even though my knowledge of both topics was limited.	Oct 8, 2013 12:31 PM
6	For me, the best part is the interaction with my peers at other institutions, learning how they approach our shared set of problems.	Oct 7, 2013 3:01 PM
7	The opportunity to share experiences and thoughts with those at other research institutions. For those of us who might not have any other interaction with other NSF-associated efforts, this is a valuable opportunity.	Oct 7, 2013 11:34 AM
8	I found the secure coding tutorial very useful.	Oct 7, 2013 10:00 AM
9	The ability for researchers and operations folks to get together and compare notes is absolutely critical in maintaining both good and open communications (something that the conference was built to address). In addition meeting other people addressing similar sorts of issues can be quite beneficial in terms of shared experiences and finding out other solutions to shared problems.	Oct 7, 2013 6:58 AM
10	I liked the fact that the panels weren't just a series of short talks but rather really discussions involving the panelists and the workshop participants.	Oct 7, 2013 6:39 AM
11	Networking opportunities were the most useful.	Oct 7, 2013 5:44 AM
12	The secure coding practices session was useful. I learned many tricks for writing better code.	Oct 4, 2013 5:12 AM
13	The tutorial was very helpful. I also liked the keynote.	Oct 3, 2013 10:13 AM
14	The tutorials seemed useful as quick intros to technologies. I think bringing everyone together to actually establish us as a community is vital. From the discussions, it seems reasonable that we can be a community and as such, can present a coherent strategy and set of plans for dealing with our security concerns.	Oct 3, 2013 6:46 AM
15	Like many other meetings, the hallway track was the most useful.	Oct 3, 2013 5:25 AM
16	The final working group was good, lots of useful discussion. Some starting points on sharing expertise from large sites to smaller sites.	Oct 3, 2013 4:26 AM
17	The assurance and federation talks were helpful. I just wish there was more	Oct 2, 2013 6:16 PM





Q12. Were there any aspects of the summit you found particularly useful or important? If so, please explain.

practical information given. I cannot honestly say I came out capable of doing anything, but start plowing through a list of websites, papers, and web searches.

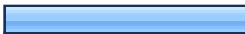



18	The day 3 session on cybersecurity programs and planning.	Oct 2, 2013 10:26 AM
19	Hearing about issues/solutions of other projects.	Oct 2, 2013 10:26 AM
20	I did not hear anything groundbreaking in the secure coding meeting. It was useful to hear everything again. I would appreciate a more in depth session, however I realize that there is likely not enough time to go into more depth.	Oct 2, 2013 7:11 AM
21	The hands-on section with the virtual machine running Bro was excellent.	Oct 2, 2013 7:10 AM
22	Learning more about various science projects and their cybersecurity implications.	Oct 2, 2013 6:53 AM
23	The workshops on the first day. I could easily see the NIDS topic expand to a whole day.	Oct 2, 2013 6:40 AM

Appendix G
Tutorial Evaluation Survey Summary Report

1. Which tutorial did you attend?

		Response Percent	Response Count
Building a Cybersecurity Program		40.9%	9
Bro Network Intrusion Detection		27.3%	6
Secure Coding Practices		13.6%	3
Streamlining Collaboration with InCommon and Identity Federations		18.2%	4
		answered question	22
		skipped question	0

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

		Response Percent	Response Count
Member / leader of an NSF project		36.4%	8
NSF Program Officer		0.0%	0
Campus IT Professional / CIO		45.5%	10
Cybersecurity Researcher		9.1%	2
Personnel from another federal program (NSA, DOE/ESNet, etc.)		0.0%	0
Other		22.7%	5

If applicable, please state your NSF Project and/or affiliated NSF Directorate. Other comments or clarifications are welcome.

8




answered question

22

skipped question

0

3. How would you rate your overall experience with the tutorial?

		Response Percent	Response Count
Excellent		54.5%	12
Good		40.9%	9
Average		0.0%	0
Below Average		4.5%	1
Poor		0.0%	0
		answered question	22
		skipped question	0

4. Please rate your experience with the tutorial in these areas:

	Excellent	Good	Average	Below Average	Poor	N/A	Rating Count
Quality of Presentation	63.6% (14)	27.3% (6)	4.5% (1)	0.0% (0)	0.0% (0)	4.5% (1)	22
Speakers' Expertise	63.6% (14)	27.3% (6)	4.5% (1)	0.0% (0)	0.0% (0)	4.5% (1)	22
Organization of Content	45.5% (10)	45.5% (10)	4.5% (1)	0.0% (0)	0.0% (0)	4.5% (1)	22
Room Layout / Comfort Level	40.9% (9)	36.4% (8)	18.2% (4)	0.0% (0)	0.0% (0)	4.5% (1)	22

We welcome comments to expand on your ratings.

2




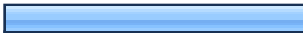

answered question

22






skipped question

0



5. Was this tutorial better than what you expected, worse than what you expected, or about what you expected?

		Response Percent	Response Count
A great deal better		9.1%	2
Quite a bit better		18.2%	4
Somewhat better		22.7%	5
About what was expected		45.5%	10
Somewhat worse		4.5%	1
Quite a bit worse		0.0%	0
A great deal worse		0.0%	0
		answered question	22
		skipped question	0

6. How useful to your work was this tutorial?

		Response Percent	Response Count
Extremely useful		31.8%	7
Very useful		45.5%	10
Moderately useful		13.6%	3
Slightly useful		4.5%	1
Not at all useful		4.5%	1
		answered question	22
		skipped question	0

7. Based on your experience, would you participate in tutorials offered at future summits?

		Response Percent	Response Count
Yes		86.4%	19
Maybe		13.6%	3
No		0.0%	0
		answered question	22
		skipped question	0

8. How can we improve this tutorial in the future?

	Response Count
	12
answered question	12
skipped question	10

9. Were there any aspects of the tutorial you found particularly useful or important? Please explain.

**Response
Count**

10

answered question

10

skipped question

12