CTSC
CENTER FOR TRUSTWORTHY
SCIENTIFIC CYBERINFRASTRUCTURE
The NSF Cybersecurity Center of Excellence

2017 Annual Report / Project Year Two

Center for Trustworthy Scientific Cyberinfrastructure
The NSF Cybersecurity Center of Excellence

NSF Grant ACI-1547272

January 1, 2017 - December 30, 2017

For Public Distribution

CTSC Team

Andrew Adams[1], Kay Avila[3], Jim Basney[3] (co-PI), Robert Cowles[5],
Jeannette Dopheide[3], Terry Fleury[3], Grayson Harbour[2], Randy Heiland[2], Elisa Heymann[4],
Craig Jackson[2] (co-PI), Scott Koranda[5], Mark Krenz[2], Jim Marsteller[1] (co-PI),
Prof. Barton Miller[4] (co-PI), Warren Raquel[3], Susan Sons[2],
Amy Starzynski Coddens[2], Von Welch[2] (PI), John Zage[3]

[1]Carnegie Mellon University/PSC

[2]Indiana University/CACR

[3]University of Illinois/NCSA

[4]University of Wisconsin-Madison

[5]Independent Consultant

About CTSC

The Center for Trustworthy Scientific Cyberinfrastructure (CTSC) is funded by NSF's Office of Advanced Cyberinfrastructure as the NSF Cybersecurity Center of Excellence (CCoE). In this role, it provides the NSF community a coherent understanding of cybersecurity's role in producing trustworthy science and the information and know-how required to achieve and maintain an effective cybersecurity program. CTSC achieves this mission through a combination of one-on-one engagements with NSF projects, training and best practices disseminated to the community through webinars, and the annual, community-building NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure.

For information about CTSC, please visit the project website: https://trustedci.org

This report describes work supported by the National Science Foundation under Grant Number ACI-1547272. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation. For updates to this report and other reports from CTSC, please visit https://trustedci.org/reports/

CTSC 2017 Highlights

A. The 2017 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure was executed by CTSC August 15-17 in Arlington, VA. Attendance was up 20% from last year with 120 people attending the summit. CTSC's presentation to the community laid out expectations for cybersecurity program governance, budgeting, and controls based on its experience.

B. We held two applications for engagements, receiving 17 total applications. The 10 applications received in 3Q2017 is a new high.

C. In addition to the NSF Cybersecurity, we hosted or co-hosted a number of workshops: one at PEARC17; URISC in collaboration with STEM-TREK at S17; a seminar for the Scholarship for Service program with Cal Poly Pomona; two Bootcamps with SGCI; and the Cybersecurity Research Acceleration Workshop and Showcase, in collaboration with Internet2, seeking to foster the transition to practice of cybersecurity research. At these events and others, we delivered 15 tutorials and 16 presentations on cybersecurity and CTSC.

D. The number of Large Facilities participating in the Large Facility Security Team rose to 22 out of 25.

E. Engagements were completed with DesignSafe-CI, the Cal Poly Pomona Scholarship for Service program, the DKIST Data Center, HUBzero, the United States Antarctic Program, MI-OSIRIS, DataONE, and the University of New Hampshire Research Computing Center. An engagement with OSG/HT-Condor was initiated and continues.

F. The Open Science Cyber Risk Profile was the subject of an IEEE Security and Privacy magazine article, a poster at the 65th ASMS Conference on Mass Spectrometry and Allied Topics, a University of California IT Blog post, and a Science Node article.

G. We added two new members to our Advisory Committee: Dr. David Halstead, CIO for the National Radio Astronomy Observatory, and Dr. Melissa Woo, Senior Vice President for Information Technology (IT) and Chief Information Officer at Stony Brook University.

H. The 12 CTSC webinars in 2017 drew more than 330 attendees and more than 750 views of the archives.

I. We published the report of the 2016 NSF Community Cybersecurity Benchmarking Survey, which has already received over 500 views: https://hdl.handle.net/2022/21355.

J. Our situational awareness service issued 14 software vulnerability alerts to 84 subscribers.

K. A citation in the NSF SI2 Solicitation (17-526) raised awareness of CTSC's services.

L. All 16 responses to our engagement evaluations indicated they were "Extremely likely" to recommend us to other projects. Our evaluations identified budgeting and resources as a barrier to impact and we made that a point of emphasis at the 2017 Cybersecurity Summit.

Table of Contents

1 Building Community

This section covers our activities to build a community that shares cybersecurity experiences, lessons learned, and effective practices in the context of NSF science.

1.1 NSF Cybersecurity Summit

The 2017 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure (https://trustedci.org/2017nsfsummit/) was executed by CTSC August 15-17 in Arlington, VA. The 2017 summit built on the success, findings, and lessons learned from previous years, and focused on the theme of Ensuring Data Provenance, Integrity and Resilience. This year the summit saw progressive growth in multiple areas. Attendance was up 20% from last year with 120 people attending the summit. Attendees included cybersecurity practitioners, technical leaders, and risk owners from within the NSF Large Facilities and CI Community, as well as key stakeholders and thought leaders from the broader scientific and information security communities. Keynote speakers included: Irene Qualters (NSF), Director of the Office of Advanced Cyberinfrastructure; Jeffrey Spies, the co-founder and Chief Technology Officer of the Center for Open Science (COS); and Marjory Blumenthal, a senior policy analyst and Director of RAND's Science, Technology, and Policy Program. This year we featured a panel on cloud security with representatives from Google, Amazon and Microsoft that allowed the CI community to discuss security strategies from commercial vendors.

Response to the Call for Participation (CFP) was the strongest in history, resulting in 15 plenary sessions, 12 training session and four table talks. Special mention of the 2017 training program is in order: this year the summit offered six parallel training sessions, the highest ever in summit history; there were 83 individuals attending the training day this year, an increase from 75 in 2016 and 45 in 2015.

Feedback for the summit and training sessions were very positive with 100% reporting the summit experience as “Excellent/Good.”

In PI Welch’s talk at the Summit,[1] he described cybersecurity expectations for the Community based on CTSC’s experiences:

Governance:

- A project should have a individual clear responsibility for cybersecurity as designated by project leadership.

[1] https://doi.org/10.6084/m9.figshare.5384155

- A project should have a set of governance documents, namely a Master Information Security Policy and Procedures (MISPP), an Acceptable Use Policy (AUP), an Incident Response Policies & Procedures, and an Access Control Policy.

Budget and Resources:

- Based on discussions at the 2016 NSF Cybersecurity Summit,[2] unless they make significant use of a parent institution's cybersecurity resources, NSF projects should have budgets for cybersecurity in the range of 3-12% of total IT budget, with the larger projects being toward the lower end of the range due to economies of scale. Projects with cybersecurity budgets below that range should carefully consider the appropriateness of their budget.

Controls:

- Projects should select and implement a reasonably scoped, prioritized, and evidence-based baseline control set (*e.g.,* the Center for Internet Security Critical Security Controls[3]). From that baseline they should work to determine the relevance, feasibility, and current implementation state of these controls and then filling gaps (*e.g.,* unique/unusual science CI) with analysis-based controls (*e.g.,* https://trustedci.org/oscrp/).

The presentation went on to discuss similar emerging expectations for software and the need to engage higher education information security offices to support cybersecurity for NSF at scale.

Training presented by CTSC at the Summit:

- Federated Identity Management for Research Organizations (full day), Jim Basney and Scott Koranda. https://hdl.handle.net/2022/21724
- Security Log Analysis (half day), Mark Krenz. https://hdl.handle.net/2022/21717
- Digital Forensics / Incident Response (half day), Warren Raquel. https://hdl.handle.net/2022/21726
- Rebuilding a Plane in Flight: Refactors Under Pressure (half day), Susan Sons. https://hdl.handle.net/2022/21719
- Developing Cybersecurity Programs for NSF Projects (half day), Bob Cowles, Craig Jackson & Jim Marsteller. https://hdl.handle.net/2022/21725
- Automated Assessment Tools - Theory & Practice (half day), Barton Miller & Elisa Heymann (included the first offering of hands-on exercises). https://hdl.handle.net/2022/21723

[2] https://hdl.handle.net/2022/21161
[3] https://www.cisecurity.org/controls/

Presentations from CTSC at the Summit:

- *Today and Tomorrow: CTSC's Services and Vision. 2017 NSF Cybersecurity Summit for Cybersecurity and Large Facilities.* Von Welch, Jim Basney, Craig Jackson, Jim Marsteller and Barton Miller. August 2017. https://doi.org/10.6084/m9.figshare.5384155
- Panel: *Cybersecurity in the Face of Overwhelming Threats.* Moderator: Von Welch (Indiana University, CTSC). Panelists: Michael Corn (UCSD); Anita Nikolich (NSF); and Kim Milford (REN-ISAC)
- *Beyond the Beltway: The Problems with NIST's Approaches to Cybersecurity and Alternatives for NSF Science.* Craig Jackson, Bob Cowles, and Scott Russell. https://hdl.handle.net/2022/21732
- *Finding Your Way in the Dark: Security from First Principles.* Susan Sons. https://hdl.handle.net/2022/21735

This year the Summit welcomed international participation with the inclusion of the WISE (Wise Information Security for E-infrastructures) community. The WISE community includes stakeholders from several large-scale distributed computing infrastructures including participants from e-Infrastructures such as EGI, EUDAT, GEANT, PRACE, XSEDE, OSG, NRENs and more.

The WISE community conducted a full day workshop during the training day open to all Summit attendees combining informational and interactive activities including:

- Introduction to WISE
- Community Projects
- Software Assurance (hands-on)
- Risk Assessment (interactive)
- Security for Collaborating Infrastructures (SCI) Self Assessment Walkthrough (interactive)
- E-Infrastructure Security Interoperability Discussion (interactive)

The WISE workshop hosted at the summit enabled the collaboration and exchange of operational practices between US and European based Cyberinfrastructure communities. More details about the event can be found on the WISE blog.[4]

Plans for next year: For the past two years we've had to decline registrations as we hit budget maximums. To accommodate growth in demand for summit attendance, in 2018 we will charge a nominal registration fee in order to increase the number of attendees. The community, by polling, has selected August 21 to 23 as the dates for the 2018 NSF Cybersecurity Summit. We will be moving the Summit to the Westin in Alexandria, Virginia.

[4] https://wise-community.org/2017/08/16/wise-feedback-gathered-at-the-nsf-summit/

1.2 Large Facility (LF) Outreach

Co-PI Marsteller attended the NSF Large Facilities Cyberinfrastructure Workshop (http://facilitiesci.org) in Alexandria, VA which took place September 6-7, 2017. Marsteller was asked to present a summary of the 2017 NSF Cybersecurity Summit at the workshop. Past and current LF activities were also shared with the attendees who were very interested in leveraging the success we have experienced with the CI community. Additionally, we were highlighted in other presenter's talks including Irene Qualters and William Miller of NSF, and Manish Parashar representing the workshop steering committee. Our involvement in the workshop spurred the request for an informational discussion with PI Von Welch and the LF CI workshop steering committee in order to learn more about our growth and community building activities. At the steering committee's request, we had a follow up call to discuss the reasons for our success and lessons learned.

Development of the Large Facilities Security Team (LFST) is progressing with 22 LFs participating of the 25 LFs identified. Starting in January, we coordinated monthly calls with the LFST that featured discussions on: the community benchmarking survey; the cybersecurity subsection of the Large Facility Manual (LFM); and various teams proposed topics covering incident response and protecting Personally Identifiable Information. In late November we asked the LFST to provide input on the structure and frequency of the meetings for 2018 and what in the LFST calls do they find most useful/valuable. The responses will shape the direction the team takes in 2018.

Considering the passage of time, and changes in both the cybersecurity landscape and our depth of understanding of the LF community, we revised our draft cybersecurity subsection of the LFM. In August, we shared the revised version with Rebecca Yasky of the NSF Large Facilities Office (NSF LFO) along with the LFST, and held a productive table talk discussion at the 2017 NSF Cybersecurity Summit. We received some insightful feedback on the draft.

Based on input from Rebecca and LF community members, we distributed a substantial rewrite of the draft to the LFST and Rebecca on December 11 . We've encouraged the LFST to review the draft and share with their management since an early draft is the best opportunity for Large Facilities to influence the document. The deadline for LF feedback is January 12, 2018.

The public comment period for the 2019 version of the LFM is scheduled for May 2018, and we expect the new cybersecurity subsection to be added to the manual.

Matt Hawkins, Head of LFO reached out to Co-PI Craig Jackson in response to the announcement of the Q1-Q2 CTSC engagement applications thanking him for CTSC's community focus and offered assistance internally with the NSF with major facility recipients.

Plans for next year: CTSC will continue to seek opportunities to engage the Large Facilities though participation in the annual NSF Large Facilities Workshop, ongoing coordination of the LFST, and continued coordination with the Large Facilities Office as the LFM work progresses.

1.3 Webinar Series

The monthly CCoE Webinar Series (https://trustedci.org/webinars/) continued into 2017. Early in 2017 we decided to post the videos to YouTube.[5] This allowed viewers to watch the recordings without having to launch Adobe Connect's on-demand application. Since we began posting videos to YouTube we've seen a dramatic increase in viewership. It is often greater (by orders of magnitude, in some cases) than the number of people who attend the presentation live.

In February 2017 we upgraded the teleconferencing license to 500 seats after two webinars hit the 100 seat registration limit.

A secondary effect of the success of the webinars has been the expanding membership to the "announcements" and "discuss" mailing lists. Attendees are asked whether they want to be added to the mailing lists during webinar registration. In 2017 we've added 94 subscribers to "announcements" and 89 to "discuss."

Table 1 on the following page shows the number of webinar attendees and archive viewers in 2017.

Plans for next year: We have decided to switch our webinar service from Adobe Connect to Zoom. January's webinar will be the kickoff presentation using Zoom. We have booked the following presenters in 2018 so far:

- **January**: Security Program at LSST with Alex Withers
- **February:** SMARTDATA Blockchain with Murat Kantarcioglu
- **March**: Data Provenance for Mobile Devices with Leon Reznik
- **April**: Creating Dynamic Superfacilities the SAFE Way with Jeff Chase and Paul Ruth
- **May**: SouthEAST SECURE with Jill Gemmill
- **July**: RSARC: Trustworthy Computing over Protected Datasets with Mayank Varia

[5] https://www.youtube.com/playlist?list=PLLoFSG1hhthQNMernoG1yT1yxeYnWkGYP

Table 1. CTSC Webinar attendance and archive viewing.

Date	Topic	Speaker(s)	Attended[6]	Watched Later[7]
Jan	Open Science Cyber Risk Profile	Welch & Peisert	37	31
Feb	Practical Cybersecurity for Open Science Projects	Jackson, Cowles & Sons	51	46
Mar	SDN & IAM Integration at Duke	Biever & Kneifel	49	125
April	HIPAA and FISMA: Computing with Regulated Data	Ramsey & Shankar	42	124
May	Technology Transfer to Practice: The NSF TTP Ecosystem	Nichols & Yasinsac	16	72
June	Using the Blockchain to Secure Provenance Meta Data	Brooks & Skjellum	30	111
July	Inaugural Security Program at Internet2	Paul Howell	27	63
Aug	Stronger Security for Password Authentication	Stanislaw Jarecki	20	44
Aug	Overview of CTSC Engagements & Application Process	Von Welch	5	43
Sept	Demystifying Threat Intelligence	Romain Wartel	15	41
Oct	Cybersecurity in an Open and Decentralized Network	Aashish Sharma	20	55
Dec	CTSC's Services and Vision	Von Welch	21	No data yet
Total			333	755

[6] Does not include CTSC staff and presenters.

[7] Either On-demand or on YouTube

1.4 Science Gateways Community Institute Partnership

We continue to partner with the Science Gateways Community Institute (SGCI, NSF award #1547611) to collaboratively fund half of a security analyst focusing on security for science gateways. CTSC made intense preparations with the SGCI Incubator team for the inaugural Bootcamp (April 24-28, 2017 in Indianapolis). The Bootcamp is a week-long intensive program for those who want to further develop and scale their gateways. A key theme is sustainability. We allowed one additional team to attend - over our initial limit of 10 as stated in 1Q2017, resulting in 23 attendees. The range of interests represented by the gateways was quite broad, including citizen science for environmental monitoring, education for biological sciences, operations research, HPC portals, and social media analysis. Overall reviews were positive. For example, when asked: How well did the Bootcamp meet your expectations? (on a scale of 1-5, with 1 being the most positive); 46% gave it a 1, 33% gave it a 2, and the remaining 21% a 3. Reviews for our cybersecurity presentation, also quite positive, are given in the Training section of this report. Our presentation was geared toward software security, with a focus on science gateway software development; however, topics related to operational security for gateways were also discussed, *e.g.*, identity management and intrusion detection. Attendees were encouraged to subscribe to the CTSC mailing lists, attend the monthly webinars, and apply for a one-on-one engagement if it made sense for their project.

Figure 1. Security presentation at the SGCI Incubator Bootcamp

The following Bootcamp (October 2-6, 2017) built on the success of the previous bootcamp by additionally facilitating a hands-on sessions whereby participants could get a better understanding of security pitfalls. This method proved to be more successful as 9 of the 10 participants agreed in the follow-up survey that they learned something that could help improve security on their gateway. The remaining participant only somewhat agreed that they learned something that could help them.

We also presented a poster[8] at the NSF SI2 PI meeting in Arlington (February 21-22, 2017). Randy Heiland attended the meeting and presented the poster which provided an overview of our activities, with a focus on our services related to software development. The meeting offered good networking opportunities with other NSF-funded project personnel.

Part of our duties in the partnership with SGCI is to help ensure the security of their web server. In the beginning, their server was using **http**; we strongly encouraged them to adopt **https**, which they did. An additional step we took in Q3 was to review their server configuration using the Qualys SSL service and pointed out some improvements that could be made. The SGCI web server administrator took appropriate action which resulted in a more secure configuration.

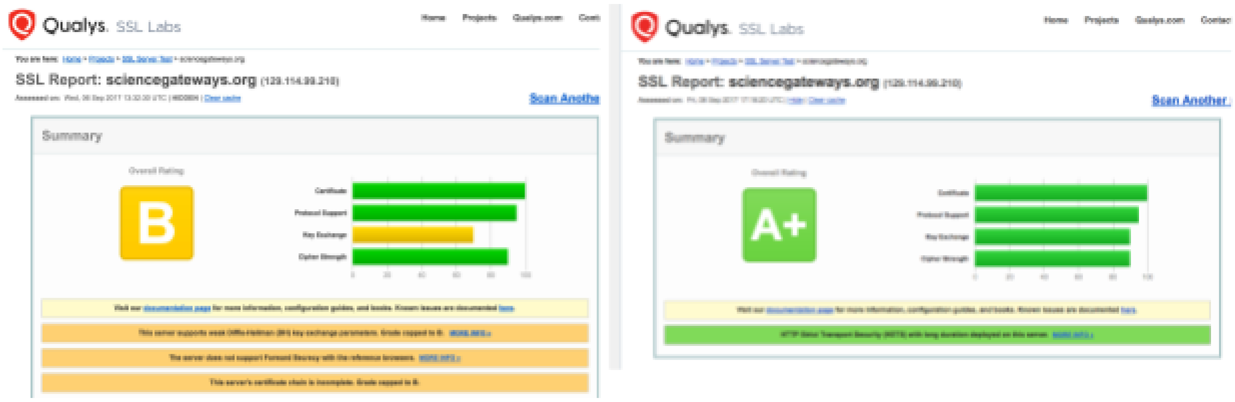

Fig 2. Improving the security of https://sciencegateways.org/

In Q3, we proactively contacted the I-TASSER (https://zhanglab.ccmb.med.umich.edu/I-TASSER/) science gateway group. I-TASSER is a heavily used gateway to perform protein structure prediction. We offered to meet with them and possibly review the security of their gateway. They let us know that, in their opinion, their university IT security group was doing a sufficient job keeping their gateway secure. In spite of this, we performed the Qualys SSL configuration test on their site and were pleased to see that it received an A- rating. Of course science gateways consist of much more than just a web server. This underlying infrastructure, in our opinion, could benefit from a cybersecurity checkup, and we plan to continue to work with I-TASSER and the broader Science Gateways community to educate them.

The end of the year brought about a transition in staffing as Randy Heiland has stepped down from the CTSC group and transitioned his role of working with SGCI to Mark Krenz, who will be holding and performing the duties of this position at .2 FTE until a permanent replacement can be determined. Additionally, in the first half of 2018, as described more fully in Section 3.1, we

[8] http://hdl.handle.net/2022/21258

will be engaging with GenApp (OAC-1740097), a key NSF project to the Science Gateway community as part of this collaboration.

Plans for next year:

- **Q1:** Provide cybersecurity consultation to a new SGCI client.
- **Q1:** Perform an audit of permissions on SGCI documents being stored in the cloud
- **Q2:** Provide cybersecurity training at upcoming SGCI bootcamp at TACC in Austin, TX.
- **Q1-2:** Engage with the GenApp project (OAC-1740097)

1.5 CC* Data: ImPACT Collaboration with RENCI

As part of its efforts in developing new ways of serving the community and exploring options for sustainability, CTSC was included by RENCI on it's ImPACT proposal to NSF, subsequently funded as award 1659367 under the CC* Data program. This award funds 10% of an analyst in CTSC over the course of the grant to provide the project with ongoing consulting and review of cybersecurity.

We plan to continue exploring similar models of offering CTSC services, experimenting with different levels of effort to determine the best model for delivering services without unreasonable overhead.

1.6 Workshop at PEARC

Fig 3. James Marsteller presenting at PEARC17.

On Thursday July 13th, we held a workshop on trustworthy scientific cyberinfrastructure at PEARC 2017 in New Orleans. Over 20 cyberinfrastructure operators, developers, and users attended the morning workshop. Von Welch started the day with an overview of NSF

Cybersecurity Center of Excellence, including CTSC's mission, vision, and engagements. James Marsteller introduced the cybersecurity challenges for smaller projects and its impact on science, followed by Jim Basney presenting the key aspects that define a cybersecurity program.

Fig 4. Von Welch and Jim Basney presenting at PEARC17.

In the second session, XSEDE's Nancy Wilkins-Diehr introduced the Science Gateways Community Institute (SGCI), which was established to provide solutions for sustaining science gateways. Von followed with a presentation on security for science gateways, concentrating on three key aspects: secure software development, identity and access control management, and operational cybersecurity. The remainder of the session was dedicated to lightning talks from workshop attendees. Internet2's Florence Hudson presented on cybersecurity research transition to practice (TTP) acceleration; a concept aimed at accelerating transitions from NSF-funded late-stage cybersecurity research into research and education environments. Tom Barton (also of Internet2) discussed the globally federated system and what support is needed for research activities. He presented a summary of the current state of eduGAIN, which connects different national federation systems across the globe. And lastly, University of Pittsburgh's Brian Stengel presented the NSF project Towards Security Assured Cyberinfrastructure in Pennsylvania (SAC-PA), which brings PA-based campus CI-practitioners, IT, and security professionals together to facilitate beneficial relationships in the region.

Plans for next year: PEARC offers us an outreach opportunity to members of the NSF community who do not attend the NSF Cybersecurity Summit. The Call for Participation for PEARC18 has been released and we have submitted a proposal to put on a similar program for next year.

Fig 5. Florence Hudson, Nancy Wilkins-Diehr, Tom Barton, and Brian Stengel presenting at CTSC's PEARC17 workshop.

1.7 Benchmarking Survey

In 2016, we began socializing and collecting responses on a benchmarking survey designed to collect and aggregate information about cybersecurity in the NSF science community. The goal was to provide the the NSF science community, CTSC, and other stakeholders a baseline view, and facilitate an understanding of changes over time. The survey included questions on topics including cybersecurity budgets, type and frequency of security incidents, and most-used best practices resources and frameworks, as well as topics suggested by the community in response for our request for input.[9]

In April 2017, we published a 38 page report analyzing the data collected in the 2016 survey, and announced the report's publication in a blog posting on May 1, 2017.[10] The document has been viewed 532 times as of December 13, 2017. We found that a total annual budget of approximately $1M was the rough dividing line in determining whether or not a project had a significant cybersecurity program. For the bigger projects and facilities there was a large variation in the size of the cybersecurity budget and we hypothesized the reasons for that variation in the report, including budget sizes driven by project mission or varying beliefs in the need for cybersecurity investment. Due to the small sample size (27 respondents, including 9 Large Facilities), we were unable to draw any strongly generalizable conclusions, but a number of observations are described in the Executive Summary section of the report and detailed in the body.

[9] http://blog.trustedci.org/2016/06/help-ctsc-build-our-community.html

[10] http://blog.trustedci.org/2017/05/2016-nsf-community-cybersecurity.html

At our all hands meeting in June 2017, we discussed a plan for improving the response rate, along with some minor tweaks to the survey to clarify responses and to gather more information on respondents reliance on host institution cybersecurity resources.

We described the major results from the 2016 NSF Community Cybersecurity Benchmarking Survey[11] during the July monthly conference call of LFST and gathered feedback.

At the NSF Cybersecurity Summit, we announced the opening of the 2017 survey (https://trustedci.org/survey) for responses. We continued to remind the LFST during monthly calls, and sent reminder emails to the Announce list and to the Summit attendee list. In an email to Matt Hawkins, we encouraged the Large Facilities Office to promote participation. When the response interval for the survey closed, we had 20 total responses including 15 responses from Large Facilities (more than a 50% increase in the Large Facility response rate).

Plans for next year: We will publish a report analyzing the data collected in the 2017 survey.

1.8 Presentations

Our outreach efforts, both to educate the community on cybersecurity for science and raise awareness of our services, included the following presentations (these are in addition to those at described elsewhere at PEARC, URISC, and the NSF Cybersecurity Summit). A list of presentations may also be found at https://trustedci.org/presentations/

- Von Welch presented a five-year retrospective of CTSC at ISI on October 30th: CTSC Five Years Later: Lessons Learned from Serving the NSF Community. Invited talk at USC/ISI, October 2017. https://doi.org/10.6084/m9.figshare.5549275.v1
- Von Welch presented an overview of CACR activities at SC17 that includes CTSC experiences: Cybersecurity and Science. Presentation at IU SC17 Booth, November 2017. https://doi.org/10.6084/m9.figshare.5687110.v1
- Jim Basney and Scott Koranda organized an IAM workshop co-located with AGU17 on December 10. http://blog.trustedci.org/2017/10/agu17.html
- Mark Krenz gave a presentation at *BroCon 2017* on September 12th on the use of awk to analyze Bro logs to detect a variety of security incidents as well as generate useful statistics. Mark also announced a new open source software tool he wrote that allows Bro users to better interface with Bro logs using awk syntax. The software is called 'bawk' and is available at https://github.com/deltaray/bawk. A recording of the presentation can be viewed at https://www.youtube.com/watch?v=20QeFkwXgCE

[11] https://hdl.handle.net/2022/21355

- Bob Cowles gave a presentation[12] to the Silicon Valley chapter of ISACA using an updated version of the “Beyond the Beltway” talk previously given at the 2017 NSF Summit. About 30 people attended from various companies in Silicon Valley.
- Von Welch. A Science DMZ in Every Pot?. *National Research Platform Workshop*, August 2017. https://doi.org/10.6084/m9.figshare.5305456
- Von Welch, Craig Jackson, Bob Cowles, Susan Sons and Scott Russell. Cybersecurity for Science. PEARC/ARCC, July 2017. https://doi.org/10.6084/m9.figshare.5193415
- Bart Miller and Elisa Heymann described how to apply their First Principles Vulnerability Assessment (FPVA) methodology to critical maritime shipping software infrastructure at the *2nd NATO Conference on Cyber Security in the Maritime Domain*, held in July 2017 at the NATO Maritime Interdiction Operations Training Center at Souda Bay on Crete.

Figure 6: Photos from the 2nd NATO Conference on Cyber Security in the Maritime Domain

- Von Welch. Cybersecurity for Science. SPAN Meeting at South Carolina State University, May 2017. https://doi.org/10.6084/m9.figshare.5028761
- Jim Marsteller. The NSF Cybersecurity Center of Excellence. Towards Security Assured Cyberinfrastructure in Pennsylvania (SAC-PA) CI Cybersecurity Workshop, June 22 & 23 2017, Wyndham Pittsburgh University Center. http://sac-pa-june-workshop.eventzilla.net/web/event?eventid=2138889726
- Jim Marsteller. Current and Future Large Facilities Impacts. NSF Large Facilities Workshop, May 3rd 2017 at LIGO Livingston & Baton Rouge. https://www.nsf.gov/attachments/190458/public/CTSC-CCoE-LFW-May-32017.pdf
- Jim Basney. Center for Trustworthy Scientific Cyberinfrastructure (CTSC) and Software Assurance Marketplace (SWAMP). CASC Spring Meeting, March 2017. https://trustedci.org/s/ctscswampcasc-170323202226.pdf
- Von Welch. Randy Heiland. CTSC Poster for NSF SI2 PI Meeting, February 2017. https://hdl.handle.net/2022/21258
- Craig Jackson. The NSF Cybersecurity Center of Excellence. Great Plains Network ENCITE Webinar, February 2017. https://trustedci.org/s/ctscswampcasc-170323202226.pdf

[12] https://docs.google.com/presentation/d/1Y2WiSHc_YtIu67WWHQD1C_xLI4cEUagd-mChRfoywmI/edit?usp=sharing

- James Marsteller. Von Welch. The NSF Cybersecurity Center of Excellence: Current and Future Large Facilities Impacts. NSF Large Facilities Security WG, February 2017. https://trustedci.org/s/CTSC-CCoE-NSF-FacSec-Feb-2017-3.pdf

Plans for next year: For 2018, our presentation plans include the following communities:

1. NSF CI Community via the NSF Cybersecurity Summit, PEARC18, the NSF Large Facility Workshop, and PI, project, and domain science meetings as we are invited (*e.g.,* SI2 PI meeting, AGU).
2. Higher education Information Security Professionals. This group interacts with research computing and research projects and our goal is to better inform them about scientific research cybersecurity via Internet2 TechEx and/or Global Summit and the Educause Security Professionals Conference.
3. Higher education research computing facilitators. These groups directly support researchers and are a good way of us having broad impact. We will present to this group via PEARC18 and regional meetings (*e.g.,* SPAN, GPN, CASC, SAC-PA).
4. Software Developers. We will continue to present to groups of software developers as the opportunity arises to promote secure software development and engineering. We are already in discussions with the SI2 PI meeting (April 30-May 1, 2018) organizers and are optimistic about presenting at that meeting.

1.9 Cybersecurity Research Acceleration Workshop and Showcase

On October 11th we co-hosted the Cybersecurity Research Acceleration Workshop and Showcase in Indianapolis with Florence Hudson of Internet2 under funding of her award (EAGER #1650445). Eighteen cybersecurity researchers from thirteen universities presented their research to attendees that included higher education CIOs, CISOs, and their peers from government and the private sector. An opening panel of CIOs, moderated by Bruce Maas (University of Wisconsin/Internet2), explored the topic of transitioning cybersecurity research to practice. The event was covered by IU's Information Technology News[13] and IU's School of Informatics, Computer Science and Engineering[14].

Plans for next year: Transitioning cybersecurity research results into practices aligns well with long-term goals of improving the cybersecurity of the NSF community and we will look for similar opportunities to foster transition to practice in the future. We believe this collaborative event was a successful way to broadly disseminate our expertise and lead the community in cybersecurity for science. We continue to seek out similar opportunities in the future.

[13] https://itnews.iu.edu/articles/2017/iu-hosts-cybersecurity-workshop-to-help-opposites-attract.php

[14] https://csi.soic.indiana.edu/2017/12/06/hillpresentation/

1.10 URISC Workshop

We co-hosted with STEM-TREK the Understanding Risk in Shared Cyberecosystems (URISC) workshop,[15] in Denver, co-located with SC17, November 11-16. The workshop presented a day and a half of training on cybersecurity and HPC presented by CTSC staff and invited experts including Florence Hudson (Senior Vice President and Chief Innovation Officer of Internet2), Susan Ramsey (Systems Security Engineer at NCAR), Thomas Sterling (Professor of Electrical Engineering and Director of the Center for Research in Extreme Scale Technologies/CREST at Indiana University), and Nick Roy (Director of Technology and Strategy at InCommon). The goal of the workshop was to provide HPC and cybersecurity education to underrepresented communities. We had twelve attendees from the South African region and nine from EPSCOR states.

Figure 7. Photos from the URISC workshop co-hosted with STEM-TREK and co-located with SC17. Photo credit to Elizabeth Leake of STEM-TREK.

Base funding for URISC was provided by NSF via a supplement to CTSC. STEM-TREK solicited supplemental funding for URISC via donations from Google, Corelight and SC17 (African registration waivers). Additionally, Dana Brunson, Assistant Vice President for Research Cyberinfrastructure and Director of the High Performance Computing Center at Oklahoma State University, contributed funds remaining from a similar workshop held in conjunction with SC16 (NSF #1657644) and allowed us to host 3 additional participants.

[15] http://www.stem-trek.org/news-events/urisc/

Coverage of the event included HPCWire[16], IU IT News[17], and STEM-TREK[18].

Plans for next year: We believe this collaborative event was a successful way to broadly disseminate CTSC expertise and lead the community in cybersecurity for science. We continue to seek out similar opportunities in the future.

2 Sharing Knowledge

This section covers our activities to create and distribute knowledge regarding cybersecurity in the context of NSF science.

2.1 Open Science Cyber Risk Profile

The Open Science Cyber Risk Profile (OSCRP, https://trustedci.github.io/OSCRP/OSCRP.html) is a living and published[19] document designed to help principal investigators and their supporting information technology professionals assess cybersecurity risks related to open science projects. It is the product of CTSC in collaboration with ESnet, specifically Sean Peisert and Michael Dopheide, and research and education community leaders, including: RuthAnne Bevier (Caltech), Rich LeDuc (Northwestern), Pascal Meunier (HUBzero), Steve Schwab (ISI), and Karen Stocks (UCSD).

In 2017 we continued to promote and sustain the OSCRP:

- The group delivered a CTSC webinar in January of 2017 highlighting the goals and benefits for researchers in open science in utilizing the risk profile document.
- The OSCRP was featured in a Science Node article featuring Karen Stocks.[20]
- Richard LeDuc (Director of Computational Proteomics, Proteomics Center of Excellence, Northwestern University) presented a poster “Protecting Proteomic Data Processing on the TDPortal with the Open Science Cyber Risk Profile”[21] on OSCRP at the 65th ASMS Conference on Mass Spectrometry and Allied Topics[22]. He reported noticeable impact in the project with fifteen attendees expressing interest in utilizing the document and four of them requesting additional information.

[16] https://www.hpcwire.com/2017/09/08/uriscsc17-tale-four-unicorns/ https://www.hpcwire.com/2017/11/01/longest-mile-matters-uriscsc17-coming-denver-colorado/ and https://www.hpcwire.com/2017/12/20/chpc-national-conference-pretoria-south-africa/

[17] https://itnews.iu.edu/articles/2017/promoting-cybersecurity-for-open-science-ctsc-plays-key-role-in-urisc-workshop-at-sc17.php

[18] https://www.linkedin.com/pulse/uriscsc17-understanding-risk-shared-cyberecosystems-elizabeth-leake/ and https://www.linkedin.com/pulse/uriscsc17-thank-you-elizabeth-leake/

[19] https://scholarworks.iu.edu/dspace/handle/2022/21259

[20] https://sciencenode.org/feature/mind-the-gap-how-to-speak-like-an-information-security-pro.php

[21] https://drive.google.com/a/iu.edu/file/d/0B7_9iS9naq1sRlhsUUJOdzhJQVE/view?usp=sharing

[22] https://www.asms.org/conferences/annual-conference

- The OSCRP was featured in a University of California IT Blog post.[23]
- Sean Peisert and Von Welch co-authored a article for IEEE Security and Privacy: "The Open Science Cyber Risk Profile: The Rosetta Stone for Open Science and Cybersecurity", IEEE Security & Privacy, vol. 15, no. 5, pp. 94-95, September/October 2017, https://doi.ieeecomputersociety.org/10.1109/MSP.2017.3681058
- Several enhancements/bug fixes (identified via GitHub's issue tracker) were addressed in the document, improving upon both content and readability.

Plans for next year: We will continue to perform outreach and monitor for additions or change requests to the document and address updates as needed.

2.2 Situational Awareness / Cyberinfrastructure Vulnerabilities

In 2017, we issued 14 cyberinfrastructure vulnerability alerts to 84 subscribers. During this period we also renamed the service as Cyberinfrastructure Vulnerabilities (CV) and consolidated the Software Vulnerability and Infrastructure Operators mailing lists into a single CV list.

We provide situational awareness (https://trustedci.org/vulnerabilities) of current cybersecurity threats to the cyberinfrastructure (CI) of research and education centers, including those threats which may impact scientific instruments. This service is available to all CI community members by subscribing to CTSC's mailing lists.

We monitor many sources for possible threats to CI, including:

- OpenSSL, OpenSSH, and Globus project and security announcements
- US-CERT advisories
- XSEDE announcements
- RHEL/EPEL advisories
- REN-ISAC daily notifications
- Social media, such as Twitter, Reddit (/r/netsec and /r/security), and LinkedIn
- News sources, such as The Hacker News, ARS Technica, Threatpost, The Register, Naked Security, Slashdot, Krebs, SANS Internet Storm Center, Paul's Security Weekly and Schneier

We filter these sources for software vulnerabilities of interest to CI operators and software developers. For those issues warranting notification to the CTSC mailing lists, we also provide guidance on how operators and developers can reduce risks and mitigate threats. We coordinate with XSEDE and the NSF supercomputing centers on drafting and distributing alerts to minimize duplication of effort and benefit from community expertise.

Plans for next year: We will continue to provide the Cyberinfrastructure Vulnerabilities service.

[23] http://cio.ucop.edu/helping-scientists-understand-research-cyber-risks/

2.3 Publications

- Sean Peisert, Von Welch, "The Open Science Cyber Risk Profile: The Rosetta Stone for Open Science and Cybersecurity", IEEE Security & Privacy, vol. 15, no. 5, pp. 94-95, September/October 2017, https://doi.ieeecomputersociety.org/10.1109/MSP.2017.3681058
- Robert Cowles and Craig Jackson, 2016 NSF Community Cybersecurity Benchmarking Survey Report, April 2017. Available: https://hdl.handle.net/2022/21355 (532 views as of December 13, 2017)
- Grayson Harbour, Scott Russell, Craig Jackson, and Bob Cowles, NIST SP 800-171 and its potential impact on NSF science, June 2017. Available: http://blog.trustedci.org/2017/06/nist-sp-800-171-and-its-potential.html (276 views as of December 19, 2017)
- Sean Peisert, Von Welch, Andrew Adams, RuthAnne Bevier, Michael Dopheide, Rich LeDuc, Pascal Meunier, Steve Schwab, and Karen Stocks. 2017. Open Science Cyber Risk Profile (OSCRP), Version 1.2. March 2017. https://hdl.handle.net/2022/21259
- James A. Kupsch, Barton P. Miller, Vamshi Basupalli, and Josef Burger, "From Continuous Integration to Continuous Assurance", *IEEE Software Technology Conference,* Gaithersburg, Maryland, September 2017.
- Joseph O. Eichenhofer, Elisa Heymann and Barton P. Miller, "In-Depth Software Vulnerability Assessment of Container Terminal Systems", *2nd NATO Conference on Cyber Security in the Maritime Domain,* Souda, Crete, Greece, September 2017.
- Joseph O. Eichenhofer, Elisa R. Heymann and Barton P. Miller, "An In-Depth Security Assessment of Maritime Container Terminal Software Systems", *submitted for publication,* December 2017.

2.4 Training

CTSC Training activities in 2017 continued to focused on educating the NSF cyberinfrastructure community on cybersecurity and secure software development. Specific events were:

- Jim Basney, Elisa Heymann, Ryan Kiser,[24] Bart Miller, and Von Welch presented at the URISC workshop as described in Section 1.10.

- Jim Basney, John Zage, Kay Avila, and Jeannette Dopheide presented at the CPP-CTSC SFS Cyberinfrastructure Security Workshop as part of the CPP-CTSC engagement as described in Section 3.4.

[24] Not CTSC-funded, but presenting CTSC-developed material.

- Numerous training sessions were offered at the NSF Cybersecurity Summit as described in Section 1.1.

- Great Plains Network & Greater Western Library Alliance training: Warren Raquel and Mark Krenz presented a one-day training workshop at the GPN-GWLA All Hands Meeting on June 2nd in Kansas City. The training was a two-part presentation on Computer Incident Response and Security Log Analysis. Ten people attended the training who were part of the GPN community, which is an NSF funded project. In preparation for the training, Warren and Mark refactored previous slides from CTSC and Bro training and added new material including more command examples and the situations in which they can be used. These new slide decks were recoverables used at the 2017 NSF Cybersecurity Summit to provide the same training and possibly in future training as well.

Figure 8. Photos from GPN and GWLA training.

- Bart Miller and Elisa Heymann presented a half-day tutorial on Secure Coding and Automated Assessment Tools at the *O'Reilly Security Conference* in New York City, October 2017.

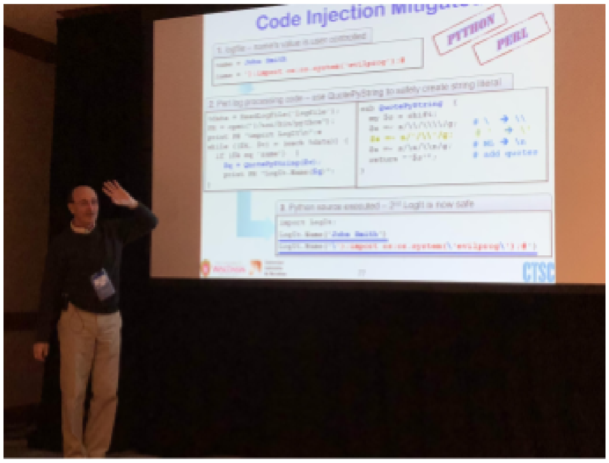

Figure 9. Photo from the O'Reilly Security Conference.

- As described in Section 1.4, we collaborated on two Science Gateways Community Institute (SGCI) Incubator Bootcamps.
- In June 2017, Bart Miller and Elisa Heymann presented an in-depth three day tutorial on secure programming and software assurance tools (including a unit on use of the SWAMP) at the FAA Technical Center in Atlantic City, New Jersey. The goal of this class was to help the FAA develop a software assurance methodology and to train their staff in these techniques. This course was based, in large part, on CTSC developed materials.

Figure 10. Photo from FAA Technical Center.

- O'Reilly Open Source Conference (OSCON).
    - Susan Sons taught a half-day tutorial on critical software and systems refactors, titled *Rebuilding a Plane In Flight: Refactors Under Pressure* at OSCON in Austin, Texas in May 2017. The tutorial was attended by 75 students and received a student evaluation score of 4.7 out of 5 stars. The training resulted in material reused at the 2017 NSF Cybersecurity Summit.
    - Bart Miller and Elisa Heymann taught a half-day tutorial on Secure Coding Practices and Automated Assessment Tools at OSCON. This tutorial was well-attended, with more than 75 students, and well-received with a student evaluation score of 4.4 out of 5.0.

SQL Injections:
attacks and mitigations
Dynamically generated SQL without validation or quoting is vulnerable
O'REILLY
OSCON
O'REILLY
OSCON

Figure 11. Photos from OSCON Secure Coding tutorial.

2.5 Software Security Course Development

We continue to make progress in the development of a self-contained course on software security. This course will be suitable for professionals in the CI community or industry, and also have application to a university curriculum. In addition to expanding the modules we use in our tutorials, we have developed the six video course modules[25] covering the topics of Pointers and Strings, Exceptions, Serialization, Numeric Errors, XML Injections, and SQL Injections, including closed captions in English for all modules.

We also continue to produce written chapter text material to accompany video modules. These chapters are being written in collaboration with Loren Kohnfelder (whose accomplishments include devising the idea of digital certificate back in the 1970's and one of the developers of Microsoft's Threat Modeling methodology). To date, we have produced chapters for the modules on Pointers and Strings, Serialization, and Exceptions.

As part of the public presentation of this material, we have developed a prototype of our online virtual book containing the body of of software assurance videos and chapters. This prototype can be found at https://research.cs.wisc.edu/mist/SoftwareSecurityCourse/.

We continue to develop practical (hands on) exercises for our courses. These first exercises provide practical experience with automated assessment tools for C/C++ and Java, using several tools through the SWAMP. More recent exercises include additional Java and web exercises, with support for programmers on Windows.

Plans for next year: The main activities for next year will be to continue to record new video modules, write the associated text chapters, and produce the hands-on exercises to accompany each module. In addition, we will produce the first Spanish language captions for our existing video modules and develop virtual machine and container packaging for our exercises.

[25] https://vimeo.com/user62215142

2.6 Guide v2

We have initiated a major revision of our "Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects" (https://trustedci.org/guide). In addition to making the Guide more modular and easier to maintain, we hope to substantially improve its scope and quality of content, consistency, and usability for a broad range of NSF projects. In the latter half of 2017, we conducted research into our design options, identified content requirements, and outlined the core content.

Plans for next year: In 2018, we will focus our efforts on content production, structural design, community feedback, and implementation. We anticipate publishing the new Guide prior to the 2018 NSF Cybersecurity Summit.

2.7 Secure Software Engineering Guide

Funded by a supplement from NSF to bolster CTSC software security efforts, we will begin working on a CTSC Software Engineering Guide in 2018. Currently, no agreed-to or widely implemented software quality or assurance standards exist. This gap places the entire secure software engineering burden of bounding the question, defining acceptable thresholds, evaluating, developing, and deploying software to those deploying and developing it. This guide will seek to eliminate this duplication of effort by providing a set of touchstone guidelines that NSF research and cyberinfrastructure projects can work from when developing software. Similar in format to the Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects (see Section 2.6), which covers operational cybersecurity needs for NSF-funded projects, this new guide would enable projects and organizations throughout the NSF community to create or improve their own programs of software engineering and assurance in order to create software that is "reliable, robust, and secure".

2.8 Broader Impacts

Broader impacts of CTSC in 2017 included:

- PI Welch represented CTSC at the Best Practices In The IoT Workshop, August 3-4 in Seattle WA[26].
- PI Welch represented CTSC at the National Research Platform Workshop, August 7-8 in Bozeman MT[27].
- Co-PI Marsteller represented CTSC at the NSF Large Facilities Cyberinfrastructure workshop (http://facilitiesci.org) September 6-7th in Alexandria, VA.

[26] https://iot.soic.indiana.edu/iot-nsf-workshop/

[27] http://prp.ucsd.edu/events/the-first-national-research-platform-workshop

- As a collaborative effort between CTSC and the DHS SWAMP project, Bart Miller and Elisa Heymann taught a three-day course on Secure Coding Practices and Automated Assessment Tools at the FAA Technical Center in New Jersey in June 2017. This course was attended by 10 technical staff members from the ground systems (air traffic control) group, who in charge of evaluating software produced by contractors for the FAA. This course is notable because it was our first course that included hands-on exercises in the use of software assurance tools (and use of the SWAMP).
- Science Node published “Mind the gap: Speaking like a cybersecurity pro”[28] covering the Open Science Cyber Risk Profile.
- Tim Howard presented on the U.S. Antarctic Program’s engagement with CTSC at the NSF FacSec working group meeting in February.
- The NSF SI2 Solicitation[29] mentioned CTSC as a resource for collaboration.
- Science Node hosted a Facebook Live interview with Susan Sons on the changing landscape of internet privacy.
- Bart Miller gave an invited lecture on Software Assurance at Carthage college, in Wisconsin, March 2016.
- Elisa Heymann and Bart Miller gave a pair of invited lectures on Software Assurance at the University of Utah in October 2017.
- Bart Miller and Elisa Heymann taught a 4-hour tutorial on Software Assurance and Secure Programming at the Universidad de la República, in Montevideo, Uruguay, with 200 attendees and extremely positive feedback. March 2016.
- Bart Miller gave an invited lecture on Software Assurance at the Georgia Institute of Technology, December 2017.

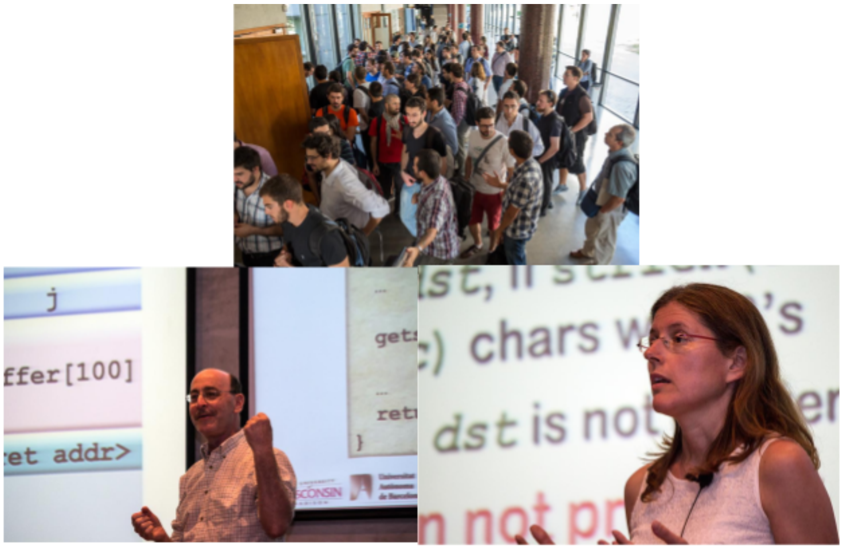

Figure 12. Pictures from the tutorial at the Universidad de la Republica in Uruguay, based on CTSC-developed materials.

[28] https://sciencenode.org/feature/mind-the-gap-how-to-speak-like-an-information-security-pro.php

[29] https://www.nsf.gov/publications/pub_summ.jsp?ods_key=nsf17526

3 One-on-One Collaborations (Engagements)

This section covers our engagements, that is collaborations with specific NSF projects and facilities to tackle their specific challenges with cybersecurity in the context of NSF science.

3.1 Engagement Applications

In 2017, the number of applications received grew and continued to significantly outrun our capacity to conduct these intensive collaborations. As such, the application process is increasingly competitive.

Table 2. Engagement Applications Received and Accepted

Round	Execution Period	Applications Received	Applications Accepted
1	1st Half of 2017	9	5
2	2nd Half of 2017	7	3
3	1st Half of 2018	10	6[30]
	Totals:	***26***	***14***

Round 1. In 2Q2016, due to demand for engagements surpassing our ability to undertake them, we deployed a new engagement application process (https://trustedci.org/application). In the second half of 2016, we received 9 applications. In that first round, we accepted the following 5 applications for engagement in the first half of 2017:

- TransPAC (NSF IRNC Award 1450904)
- OSiRIS (CC*DNI DIBBS Award 1541335)
- DataONE (ACI, CSE #1430508; previously ACI #0830944)
- University of New Hampshire Research Computing Center (CC*DNI, Grant #1541430)
- HTCondor-CE (PHY-1148698)

Round 2. In 1Q2017, we executed our second engagement application round. We received 7 new applications, and considered a total of 8 applications (including one deferred from late 2016) for engagements in the second half of 2017. We accepted 3 new engagement applications:

- Cal Poly Pomona Scholarship for Service Program (1504526)
- Design Safe (NHERI: CI-1520817)

[30] 4 applicants agreed to a combined engagement

- DKIST Data Center (AST-0946422)

In 2Q2017, we received negative, constructive feedback from an applicant regarding the quality and clarity of our communication. As a result, we substantially revised the criteria by which we evaluate applications, as well as our communications process.

Round 3. In 3Q2017, we opened and socialized the application (trustedci.org/application) for engagements to be executed in 1H2018, with an updated application form and process to reflect lessons learned from prior rounds. We received 10 applications, and accepted 6 applications for execution in the first half of 2018:

- National Radio Astronomy Observatory (AST-1647378)
- GenApp (OAC-1740097)
- Cloud Best Practices (combining 4 applications):
    - The Agave Platform (OAC-SS2-SSI-1450437)
    - Cornell University Center for Advanced Computing (ACI-1541215 CC*DNI DIBBs; ACI-1548562)
    - CyVerse (DBI-0735191)
    - Jetstream (1445604)

For a summary of all our planned, current, and past engagements, see Table 4 and Table 5.

Plans for next year: In early 1Q2018, we will finalize detailed planning and begin execution of our 3 new engagements. We also will open and publicize a call for applications for engagements to be executed in the second half of 2018.

3.2 Consultations

One of the ways we serve the community is through a number of ad hoc discussions and answering of questions. These “consultations” normally take the form of a phone call, a in-person discussion in a hallway at a conference, or an email exchange. We expect in aggregate they represent a significant contribution to the community.

In 3Q2017 we started to more formally log these consultations and attempted to broadly distribute the results through blog posts. We logged four consultations with the NSF Chameleon project, DKIST/NSO (distinct from our full engagement with DKIST Data Center), FIU International Hurricane Research Center, and the Oklahoma State High Performance Computing Center.

One blog post resulted:
http://blog.trustedci.org/2017/09/ask-ctsc-questions-for-leadership-to.html

Plans for next year: We will continue to track consultations and broadly disseminate their results through a blog posts.

3.3 Cal Poly Pomona Scholarship for Service

On the weekend of October 14th, the California State Polytechnic University Pomona Scholarship for Service program in collaboration with us hosted a cyber workshop[31] for Scholarship for Service (SFS) students. A total of 45 students from 13 different universities traveled to Pomona, CA. The students spent all day Saturday and half of Sunday participating in workshops covering topics such as public key infrastructure and deployment, log analysis + Splunk, network security in a Science DMZ, and federated identity and access management.

The students who attended this workshop were participants of the Cybercorps Scholarship for Service (SFS) program, designed by the National Science Foundation to strengthen the workforce of information assurance professionals protecting the government's critical information infrastructure. The Scholarship for Service (SFS) program is a partnership between the Department of Homeland Security and the NSF to grant 4-year colleges scholarship funds to encourage students to pursue cybersecurity as a career. Scholarship recipients agree to work for a qualifying federal or state government agency upon graduation as a means of returning the investment in their education with the additional benefit of strengthening critical government infrastructure. Cal Poly Pomona (CPP) received such a grant in 2015 (NSF award #1504526) and its program is headed by Professor Mohammad Husain.

The engagement process started in May of 2017, with CPP submitting an application requesting assistance in creating a training workshop for the SFS students. Once the engagement started, we shared equally with CPP the task of planning the event. Cal Poly Professors Dr. Mohammad Husain, Dr. Ron Pike, and Dr. Tingting Chen, as well as CTSC security professionals Dr. Jim Basney, Jeannette Dopheide, John Zage, and Kay Avila participated in the coordination. As a base for the lessons, we used materials from our previous lectures and training, created new material, and prepared hands-on training in a single virtual machine from the NSF project SEED base image. We archived the workshop materials at https://hdl.handle.net/2142/98520.

Student survey responses indicated that the hands-on sessions were well received, especially the log analysis session. Ninety-five percent of students found the workshop either good or excellent, while sixty-three percent thought they were more likely to pursue a career in cyberinfrastructure security after the workshop. The response from the engagement evaluation from CPP was also overwhelmingly positive, making note of effective communication between CPP and CTSC including collaboratively setting the agenda, meeting minutes, and to-do lists during the engagement.

[31] https://www.cpp.edu/~polysec/ciworkshop2017.html

Plans for next quarter: We will release CTSC-CPP SFS workshop videos on the CTSC YouTube channel[32] for community use.

3.4 DesignSafe-CI

We completed our engagement with DesignSafe-CI (DesignSafe)[33], a component of the Natural Hazards Engineering Research Infrastructure (NHERI)[34] and funded by the NSF under a Cooperative Agreement through the Division Of Civil, Mechanical, and Manufacturing Innovation (CMMI)[35] (NSF-1520817)[36]. In a cyber-checkup tailored for DesignSafe's existing NIST 800-53 based cybersecurity control implementation, we reviewed security documents for DesignSafe and seven experimental facilities (EFs) DesignSafe governed, and then generated a matrix in order to display the thoroughness of each site's adherence to best practices in security. Using this observed data, we collaborated with DesignSafe in identifying opportunities for improvement for each of the sites' existing security programs.

We learned in follow-up discussions with DesignSafe that they have already begun implementing improvements highlighted by the gap analysis from our matrix. Moreover, DesignSafe has already responded to and completed our engagement evaluation questionnaire.

Plans for next year: We will continue to monitor DesignSafe's progress and respond to any queries they may have in 1Q2018.

3.5 DKIST Data Center

We completed a six month engagement with the DKIST Data Center (NSF AST-0946422[37]) with the goals of assisting the DKIST Data Center team in the development of a cybersecurity plan and providing them with recommendations for security training based on their needs. The DKIST Data Center, located in Boulder on University of Colorado's east campus, serves as the operations data management and processing center for the Daniel K. Inouye Solar Telescope (DKIST[38]) in Haleakala on Maui, Hawai'i. Coinciding with the beginning of the engagement and its planning, the NSF Cybersecurity Summit provided our engagement team an opportunity to meet with the DKIST team and learn from them about their plans for the data center. The discussion at Summit also allowed our team to better understand the relationship between the DKIST Data Center in Colorado and the DKIST telescope in Hawaii. DKIST Data Center staff

[32] https://www.youtube.com/channel/UCD2sZ957eokDw8mcjkHXvXw
[33] https://www.designsafe-ci.org/about/designsafe/
[34] https://www.designsafe-ci.org/about/
[35] https://www.nsf.gov/div/index.jsp?div=CMMI
[36] https://www.nsf.gov/awardsearch/showAward?AWD_ID=1520817
[37] https://www.nsf.gov/awardsearch/showAward?AWD_ID=0946422
[38] http://dkist.nso.edu/

explained the purpose of the data center and their responsibilities in securing the flow and storage of the data from the telescope.

After developing an approved engagement plan, we began weekly meetings to start work on the cybersecurity plan. In total the combined team created 11 cybersecurity policies and procedure documents based on the templates available from trustedci.org. As part of the process for developing these policies and at the request of the DKIST team, our team reviewed the policies of the parent and affiliate organizations (NSO, AURA and Univ. of Colorado) and determined how they apply and how to align DKIST policies with those existing policies. The policy development process also provided another chance for us to review the application of the Guide templates and encouraging feedback on potential improvements.

To achieve the second goal of the engagement, throughout the course of the engagement the we identified appropriate security training for various staff roles on the DKIST team. Toward the end of the engagement, the CTSC engagement team made a site visit to DKIST's facility in Boulder, Colorado. This face-to-face opportunity facilitated communication as we finalized the development process of the security policies and reviewed all the policies written during the term of the engagement. Additionally, we performed a physical review of the data center and a co-located center, provided a tutorial on the risk analysis process, and guided the DKIST staff through a tabletop cybersecurity exercise. DKIST also presented their current network map and demonstrated their current installation and security compliance tools.

Our final report to the DKIST Data Center staff included a summary of the activities and deliverables developed during the engagement and nine recommendations we believe would be high impact improvements to the security of the DKIST Data Center if they are implemented. We based these recommendations on observations made both during the site visit and in the overall course of the engagement.

3.6 Open Science Grid / HTCondor-CE

We continue our First Principles Vulnerability Assessment[39] (FPVA) engagement with The Open Science Grid (OSG, NSF PHY award #1148698)[40] to assess the security of HTCondor-CE (Compute Element) (NSF ACI award #1321762). As of Q3 we completed the Architectural (Component), and Resource diagrams, including privilege (`user`, `root`, other) information and moved to step 4 of the methodology -- the detailed code inspection and analysis for vulnerabilities.

In October 2018, we started a new student from UW-Madison on this assessment effort, Sanjay Rajmohan. He installed a new testbed at the University of Wisconsin, and then spent time getting up to speed on HTCondor-CE and reviewing the work done by previous students. Sanjay

[39] https://research.cs.wisc.edu/mist/papers/VA.pdf
[40] https://www.opensciencegrid.org/

then started running initial tests on a testbed he installed, aimed at investigating if a user process could leave an undetected child process on the PBS executing machine. While that was not possible, a user process running on an executing machine could attack another user processes if both execute at the same time on the same machine.

Plans for next year: In the upcoming weeks, we will continue to run different tests with the objective of exploiting critical resources.

3.7 University of New Hampshire Research Computing Center (UNH RCC)

We completed a successful engagement with the University of New Hampshire Research Computing Center[41] (UNH RCC) (funded in part by the NSF CC*DNI program, Grant #1541430) to assess and facilitate the reasonable maturation of UNH RCC's information security program and positively impact the security of the cyberinfrastructure and trustworthiness of the science UNH RCC supports. Following a period of fact-finding, we delivered a containing specific prioritized recommendations grounded in best practices for maturing the UNH RCC program. As a first time experiment, we performed the site visit more than a month after delivering the report (rather than during fact-finding), giving time to plan and conduct a period of collaborative work in preparation for the site visit where meetings, training sessions, and other activities leveraged the report to build momentum, and maximize the its positive impact.

Patrick Messer,[42] Director of the UNH Research Computing Center, stated,

> *"The engagement process with CTSC has already had a direct impact on research computing at UNH. Senior level administrative discussions have led to the inclusion of RCC staff on UNH's Information Security Services bi-weekly team meetings, bi-weekly leadership team meetings, and strategic retreats. Both the site visit and the report recommendations emphasized practical approaches to improving cybersecurity. UNH research computing now has a 12-month plan with realistic deliverables and efforts addressing the report recommendations are underway. The plan will be reviewed annually to address those CTSC recommendations that are longer term. Although the engagement focused on the cybersecurity of NSF projects, this effort can't help but positively impact the entire UNH science community. I am grateful that UNH was able to participate in the engagement process."*

Engagement Process: In the course of the engagement, UNH RCC engaged with us in ten one-hour video conference calls. These calls were primarily in the fact-finding phase of the engagement and were key to clarifying the computing environment at both UNH and UNH RCC. While web searches provided information about the publicly documented environment, a

[41] https://www.unh.edu/research/support-units/research-computing-center
[42] https://www.unh.edu/research/staff-directory/messer-patrick

number of additional documents and diagrams were made available to us. The subsequent report comprised three key sections of recommendations. The first section, titled “Recommendations for Pivotal Actions”, contained two recommendations relating to strategic actions to consider about its approach to cybersecurity in the context of the UNH system. The second section, titled “Recommendations for actions best implemented at the university level, but may remain UNH RCC’s responsibility”, contained six recommendations for high impact actions for consideration if UNH RCC maintains the status quo of relative independence from UNH IT and responsibility for its own day-to-day security practices. These recommendations ranged from selecting a cybersecurity framework to patch management and network monitoring. The third and final section, titled “Recommendations best implemented at the research computing center level”, contained seven actions for consideration regardless of the disposition of the pivotal decisions. These recommendations ranged from asset inventory to change control and developing a core information security policy. Throughout the report we made frequent reference to The CIS Critical Security Controls for Effective Cyber Defense,[43] and also referenced the Australian Signals Directorate's Essential Eight.[44]

UNH RCC organized and facilitated our site visit. We met with a wide range of stakeholders, including the UNH SVP for Research and the UNH CIO, the faculty advisory committee (plus interested researchers), general counsel, and the UNH RCC software development team. Many meetings included not only the engagement team, but also representatives from the UNH IT cybersecurity team. Topics for the meetings included: addressing contractual requirements for protecting Controlled Unclassified Information; developing an Acceptable Use Policy; Freedom of Information Act considerations; and both overview presentations and detailed discussions of the recommendations in the report. We also presented new material on selecting cybersecurity frameworks and control sets, and the group delved into implementation details of the Critical Security Controls.

In the wake of this site visit, UNH RCC prepared a “summary of the plans for implementing cybersecurity recommendations that resulted from a UNH collaboration with the Center for Trustworthy Scientific Cyberinfrastructure (CTSC)”. In addition to meetings at the university level regarding funding and integration with UNH IT, the summary described plans for implementation in six- and twelve-month timeframes to improve cybersecurity for the three categories of UNH RCC systems. In their 6-month update, UNH RCC stated, “due to the CTSC engagement momentum and the ripe UNH environment for IT security enhancement, RCC has made our CTSC security response [the] Wildly Important Goal (WIG) for this fiscal year,” and they reported significant progress in all areas of the recommendations from the CTSC report.

[43] https://www.sans.org/critical-security-controls
[44] https://asd.gov.au/publications/protect/essential-eight-explained.htm

Plans for next year: We will track progress via the engagement evaluation questionnaire and follow-up phone calls at the timeframe intervals in the implementation plan UNH RCC developed.

3.8 DataONE

We engaged DataONE (ACI, #1430508)[45] in a cyber-checkup -- a high-level review of a project's cybersecurity program -- to produce a list of opportunities that described new or updated mechanisms and/or policies that DataONE could undertake in order to strengthen and advance its cybersecurity posture. In our follow-up conversation, DataONE reported they had begun implementing three of the opportunities identified in our report (i.e., centralized log processing, nIDS and improved coverage of security documents), adding that others would be addressed as more resources became available.

3.9 HUBzero

In 2016, CTSC engaged with HUBzero (NSF award #1227110)[46] to aid them in maturing their information security program in the face of an internal reorganization, work which wrapped up in January 2017. Since then, HUBzero has accepted and integrated the Master Information Security Policy and Procedures document we helped it develop, and they used some of our guidance to formalize security-critical software engineering practices and address security as early in the R&D process as possible.

In Q3 2017, we circled back to find out how this work has impacted HUBzero. HUBzero's responses to our post-engagement survey showed that the engagement's impact was generally positive, but that more could have been done with additional effort and attention from some key personnel at HUBzero. The HUBzero Information Security Officer also specifically requested that we publish general guidance on software engineering practices for scientific CI projects that develop software. Given that guidance, projects can prepare more on their own and become more mature before going into a CTSC engagement. We anticipate that the upcoming CTSC Software Engineering Guide for NSF Science and CI Projects will help fill this need.

3.10 TransPAC

We completed our engagement with the IRNC TransPAC project (NSF Award #1450904),[47] assisting them in developing a cybersecurity plan and program based on our Guide (https://trustedci.org/guide).

[45] https://www.dataone.org/
[46] https://hubzero.org/
[47] http://internationalnetworks.iu.edu/initiatives/transpac/

Plans for next year: We are awaiting the TransPAC project's response to our survey in order to gauge the engagement's impact.

3.11 Multi-Institutional Open Storage Research Infrastructure

Representatives of the MI-OSiRIS[48] project (NSF ACI award #1541335) submitted an application in June 2016 requesting a joint design review of the OSiRIS Access Assertion (OAA) system. We conducted the engagement from October 2016 to March 2017 via a series of hour-long phone calls with OSiRIS staff to discuss and review the OAA design. OAA design documents[49] were the primary source materials used in the review. At the time of the review, the OAA system was in an early design and implementation phase, giving the group the opportunity to consider a variety of design options and give input to design decisions, in contrast to an after-the-fact security evaluation of an implemented system.

The engagement team discussed two categories of use cases for the OSiRIS system: 1) distributed access to scientific data using Ceph[50] and 2) network discovery, monitoring, and management using perfSONAR[51] for reliable and high-performance use of Ceph across the network. The OSiRIS design includes a common authentication and authorization mechanism across these use cases, supporting federated campus authentication via Internet2's InCommon[52] service and group-based access control (with delegated sub-groups) using Internet2's COmanage[53] software.

The OAA system uses concepts from OAuth (RFC 6749), including JSON Web Tokens (RFC 7519) and the practice of issuing shorter-lived access tokens and longer-lived refresh tokens. This fact inspired the engagement team to use the OAuth 2.0 Threat Model and Security Considerations (RFC 6819) as an evaluation framework for the OAA system. In applying the RFC 6819 Threat Model to the OAA design we made number of observations, most of which have already been incorporated into the evolving OAA design. The final engagement report includes a set of security recommendations that the OSiRIS project plans to implement in its deployed cyberinfrastructure. We identified no significant weaknesses in its review of the initial design of the OSiRIS access control system.

4 Engagement Evaluations

Since August of 2016 we have routinely followed up with prior engagements to assess long-term impact and our own engagement processes. We have received 16 responses to our

[48] http://www.osris.org/
[49] https://github.com/MI-OSiRIS/aa_services/tree/master/doc
[50] http://docs.ceph.com/
[51] https://www.perfsonar.net/
[52] https://incommon.org/federation/
[53] https://www.internet2.edu/products-services/trust-identity/comanage/

Engagement Evaluation Questionnaire[54] to date, including 11 responses in 2017. This section begins with a summary of those responses in the aggregate, and then provides some analysis of select individual responses.

4.1 Engagement Evaluation Summary Analysis

We consistently see high ratings of the positive impact of the engagement on the project or facility, and all 16 responses show a 5 out of 5 ("Extremely likely") to Question 7: "How likely are you to recommend that other researchers, projects, or facilities engage with CTSC?"

However, not every response indicates maximum positive impact. Several respondents identified barriers to the engagement having more positive impact, mostly commonly selecting "Other priorities diverted attention from cybersecurity" and "Insufficient staff/budget/resources to make recommended changes." Recognizing that insufficient budgeting and resources for cybersecurity in NSF projects is a common challenge, it was a point we emphasized at the 2017 NSF Cybersecurity Summit, and we added managerial and resource commitment as a point of emphasis in our Engagement Application Process described in Section 3.1.

The 16 responses include 13 first time evaluations, 3 first follow-up evaluations, and 1 second follow up evaluation. We target follow-up evaluations at 6 month intervals for at least two follow-up evaluations. The individual follow-up responses have not yet shown a pattern of substantial change over time. We include all 16 responses in the aggregated summaries below for ease of analysis and to represent the full data set.

Q1. On a scale of 0 - 5, rate the positive impact of the engagement on the project or facility.

11 of 16 responses were 5. All 16 responses were 3, 4, or 5.

Q2. On a scale of 0 - 5, rate the negative impact of the engagement on the project or facility.

Only 1 response indicated any negative impact, with a rating of 1.

Q3. How has this engagement improved cybersecurity for your project or facility?

Respondents were able to select multiple items among 14 options (including "This engagement has not improved cybersecurity for the project or facility") or enter an "other" response. All positive responses were selected at least once.

The most frequently selected responses were:

- Improved governance / policy / risk acceptance structure (10)
- Increased cybersecurity knowledge among staff and personnel (10)
- Knowledge / documentation of information assets (9)
- Communication of risks to decision-makers and stakeholders (9)
- Understanding cybersecurity risks to the science mission (8)

[54] https://goo.gl/forms/VHL8Gtda2nWMgu9H3

- Selection of better technology or services (8)

Q4. Which improvement has had the most impact on the cybersecurity program?

5 responses indicated "Improved governance / policy / risk acceptance structure."
4 responses selected "More security or efficient identity and access management."

Q5. Have there been barriers to this engagement having a more positive impact?

Respondents were able to select multiple items among 10 options (including "None") or enter an "other" response.

8 responses selected "None."
5 responses selected "Other priorities diverted attention from cybersecurity."
3 responses selected "Insufficient project or facility resources applied to engagement."
3 responses selected "Insufficient staff/budget/resources to make recommended changes."

Q6. Which one of the barriers was most significant?

3 responses selected "Other priorities diverted attention from cybersecurity."
3 responses selected "Insufficient staff/budget/resources to make recommended changes."

Q7. How likely are you to recommend that other researchers, projects, or facilities engage with CTSC? (0 = Not Likely; 5 = Extremely likely)

All respondents selected 5 ("Extremely likely").

Q8. Did the engagement with CTSC increase understanding within your project or facility of the role of cybersecurity in producing trustworthy science? If so, how much? (0 = No increase; 5 = Great increase)

We received 4 ratings of 5. 15 of 16 responses were 3, 4, or 5.

Q9. How does the CTSC engagement compare to other cybersecurity-related assistance or services your project or facility has received?

Respondents were asked to rate the CTSC engagement along 4 variables. The responses generally indicate that engagees believe they receive superior service from CTSC.

- **Usefulness**. 9 ratings of "much better"; 4 of "somewhat better"; 2 of "about the same".
- **Quality of communication**. 7 ratings of "much better"; 5 of "somewhat better"; 3 of "about the same".
- **Quality of deliverables**. 8 ratings of "much better"; 5 of "somewhat better"; 2 of "about the same".
- **Positive impact on security**. 8 ratings of "much better"; 4 of "somewhat better"; 2 of "about the same".

Q10. Have any other projects, facilities, or professionals (outside your project or facility) been positively or negatively impacted indirectly by this engagement? If so, please explain.

> 10 of 15 responses indicated some positive impact broader than the immediately engaged organization (*e.g.,* sibling organizations, campus IT, customers for services offered).

Q11. How can CTSC increase the positive impact of its engagements?
Q12. How can CTSC improve its engagement processes and products?

> Responses to Questions 11 and 12 have influenced not only our engagement practices, but also efforts in other areas (such as the Guide revision and assistance to NSF in drafting the future cybersecurity section of the Large Facilities Manual). These include more effort at helping NSF projects and facilities prioritize effort.

Plans for next year: We will continue to utilize the Engagement Evaluation Questionnaire as one method to measure impact, identify areas for improvement and innovation, and better understand the community we serve. We will place more emphasis on detailed follow-up interactions in our new engagement plans. We continue to lag on receiving requested responses from some prior engagees, and will add additional emphasis as we initiate new engagements in 2018.

4.2 Gemini Observatory Evaluation Analysis

The following comments were included in the response to the six-month follow-up to our engagement with the Gemini Observatory.

> *Having the report, and detailed recommendations allowed the process to survive multiple management and cybersecurity team staff changes. Our security posture, policy framework and overall cybersecurity program have improved considerably as a result of the engagement.*
>
> *For centers and organizations that don't have resources (be that in staff or budget) to follow up on the recommendations from the engagements, offering a potential roadmap that could be presented to management might facilitate the process once the engagement has been completed.*

In the twelve-month follow-up, Gemini reported that staffing issues had been a limiting factor in implementing the recommendations; however, resources have now been assigned to cybersecurity initiatives and they are actively working on implementing our recommendations.

4.3 United States Antarctic Program (USAP) Evaluation Analysis

Comments from six-month follow-up of the engagement with USAP also indicated budget and staffing issues affecting their ability to implement the recommendations contained in the engagement's final report. They are still evaluating how to approach implementing the recommendations.

4.4 SciGaP Evaluation Analysis

In our follow up with SciGap (NSF Award #1339774), PI Marlon Pierce, in addition to positive feedback, provided the following constructive suggestion:

> **How can CTSC improve its engagement processes and products?**
> Response: "Provide more resources for more but less intensive consultations."

We are exploring a variant of our normal six month engagement model to provide for longer-term, less intensive support.

5 Lessons Learned, Challenges, and Project Management

In this section we cover unexpected changes to the project as well as lessons learned.

5.1 Sustainability

We are working towards a vision of being fiscally supported directly by NSF, indirectly by NSF projects through subawards, e.g. by SGCI as described in Section 1.4 and ImPACT as described in Section 1.5, and ultimately non-NSF projects when such support would not detract from our mission of supporting the NSF community and NSF science. The support by SGCI and ImPACT are significant steps in this direction in that they demonstrate our perceived value by the community and we will continue refining our model of providing service, drawing on lessons learned from the individual project members in supporting other NSF projects (e.g. IU, NCSA and PSC between them support the Open Science Grid, LSST, and XSEDE, and the University of Wisconsin does software evaluations of other projects[55] as well).

5.2 Supplements from NSF: URISC, Software Security, and REU

CTSC received three supplements from NSF in 3Q2017. One was for the URISC workshop as described in Section 1.10. The second supplement was to boost CTSC's efforts in Software Security as described in section 2.7. The third was a Research Experience for Undergraduate (REU) supplement to fund students at IU and University of Wisconsin. The REU funding arrived

[55] See http://research.cs.wisc.edu/mist/includes/vuln.html

too late to fund Summer students as planned and in consultation with NSF was repurposed. At IU the funds will instead be used for a student to assist with the software security supplement. At UW-Madison, the student assisted with current in-depth software assessments, initially with OSG/CondorCE.

5.3 Common Challenge of Insufficient Cybersecurity Resources

As described in Section 4.1, we noted a common challenge of insufficient budgeting and resources for cybersecurity in project with which we engaged hindering long-term impact from our engagements. We emphasized budgeting at the 2017 NSF Cybersecurity Summit and we added managerial and resource commitment as a point of emphasis in our Engagement Application Process described in Section 3.1.

5.4 Advisory Committee Changes and Meeting

We added two new members to our Advisory Committee: Dr. David Halstead, CIO for the National Radio Astronomy Observatory, and Dr. Melissa Woo, Senior Vice President for Information Technology (IT) and Chief Information Officer at Stony Brook University. These additions represent CTSC's strategic interests in Large Facilities and working with the higher education sector to scale to support NSF science broadly. Our blog post announcing these additions[56] gives more details on Drs. Halstead and Woo. The full list of CTSC Advisory Committee members currently is:

- Tom Barton, Senior Consultant for Cyber Security and Data Privacy at the University of Chicago.
- David Halstead, CIO for the National Radio Astronomy Observatory.
- Neil Chue Hong, Director of the Software Sustainability Institute (SSI).
- Nicholas J. Multari, Senior Project Manager for Research in Cyber Security at the Pacific Northwest National Lab (PNNL).
- Nancy Wilkins-Diehr, San Diego Supercomputing Center, Director of XSEDE's Extend Collaborative Support for Communities program, PI of the NSF Science Gateway Community Institute.
- Melissa Woo, Senior Vice President for Information Technology (IT) and Chief Information Officer at Stony Brook University.

The CTSC Advisory Committee was convened on November 13th, proximate to the SC17 conference. Anita Nikolich, Kevin Thompson and Scott Sellars were invited to attend and

[56] http://blog.trustedci.org/2017/09/ctsc-welcomes-two-leading-cios-to-its.html

observe as representatives from NSF, with the latter two doing so. A set of outcomes from that meeting are being derived and will be shared with NSF once completed.

5.5 CTSC All Hands Meeting

In late June, we held our annual face-to-face All Hands Meeting in Chicago. We used the time together to complete the Study phase of our biannual Plan-Do-Study-Act (PDSA) cycle, identifying and game-planning responses to issues as well as discussing new initiatives. Major themes included our programmatic outreach effort; the range of our one-on-one engagement efforts; the balance of our engagement effort allocation versus other, potentially broader impact activities; and new ways of increasing and measuring CTSC's positive impact on the community.

5.6 CTSC Rebranding to Emphasize CCoE

In early 1Q2018 we will roll out our new logo in collaboration with the Indiana University's IT Communications Office, shifting our "Center for Trustworthy Scientific Cyberinfrastructure (CTSC)" to "Trusted CI." The goal is to emphasize the "NSF Cybersecurity Center of Excellence" title while maintaining any brand recognition in "CTSC" and avoiding confusion.

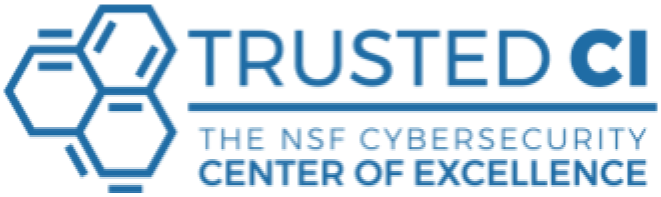

Fig 10. New CTSC Logo

5.7 Personnel changes

- At IU, Randy Heiland, who has been our analyst supporting the partnership with SGCI, departed CTSC to pursue other opportunities at Indiana University. We have therefore begun transitioning his duties to other CTSC staff and determining a long-term replacement.
- At IU, Amy Starzynski Coddens, the Education Outreach and Training Manager for CTSC, has left her position at IU and CTSC. We are planning not to replace her position and instead distribute her responsibilities to other staff.
- We welcomed two new members to the CTSC team at NCSA: Kay Avila and John Zage.
- At the end of 2017, we welcomed one new member to the CTSC team at CACR: Scott Russell.
- At IU, Susan Sons stepped away from CTSC to focus on new leadership roles with the Open Science Grid, the DHS SWAMP project, and the Internet Civil Engineering Institute, but subsequently returned to lead the Secure Software Engineering Guide efforts (Section 2.7).

6 Metrics

We have added several metrics this year, designated with the text “(new)” in the second column.

Table 3. CTSC activity goals and achieved metrics.

Activity	Measurement Technique	Goals	Achieved
Engagements with NSF projects.	Direct measurement of the number of engagements.	4-6/year depending on complexity.	On track and exceeding. Eight engagements completed in 2017 (HUBzero, USAP, MI-OSIRIS, DataONE, UNH RCC, CI-Design Safe, DKIST Data Center, Cal Poly SFS). One underway (OSG/HT-Condor).
	Post-engagement survey.	High ratings of engagement utility.	On track. See Section 3.3 for new results.
	Consultations (new)	None.	4
NSF projects using our best practices, guides, threat model to develop and maintain their own cybersecurity programs.	Reported by NSF projects.	Initially 2-4/year using cybersecurity program guide. Aim to increase linearly.	To date DKIST, Gemini Observatory, HUBzero, LSST, NCAR, Pittsburgh Supercomputing Center, UNH RCC, and TransPAC have used our Guide. The Proteomics Center of Excellence at Northwestern have used the OSCRP. We believe there is more usage and are working on a better mechanism to collect this information.
Training	Direct measurement of attendance.	50 members of NSF community per year attending.	According to sign-in sheets at the training for NSF Cybersecurity Summit, 62 NSF community members attended training, 24% more than our goal.
	Survey of attendees.	90%+ rating training as valuable.	Based on the results of a survey sent after the training, 90% of respondents answered that based on their experience that they would participate in the future. 10% answered that they may participate.

Table 3 (continued). CTSC activity goals and achieved metrics.

Activity	Measurement Technique	Goals	Achieved
Situational Awareness	Direct measurement of number of individuals and NSF projects receiving announcements.	90%+ of Large Facilities receiving announcements by end of YR1. Aim to increase linearly.	Currently 11 out of 25 Large Facilities represented on our list (44%).
	Survey of community receiving information.	75%+ of recipients rating announcements as valuable and providing information they would not otherwise be aware.	In our December 2016 survey, 85% of respondents rated the announcements as valuable and providing information they would not otherwise be aware.
Summit	Direct measurement of attendance.	90%+ participation of Large Facilities. Strong, diverse participation across the full range of NSF CI projects, and program officers.	Representation from 58 NSF projects including 18 large facilities. An increase of 14 projects and 10 large facilities over 2016.
	CFP response rate.	Increasing CFP response rate each year.	The 2017 Cybersecurity Summit CFP saw a significant increase in community responses from the previous year. 28 total presentations were submitted including 15 general presentations and panel talks and 13 training sessions. This was a 47% increase over 2016.
	Surveys of attendees.	Very strong evaluations on attendee surveys.	A post summit survey received responses from 45 attendees. To the question "How would you rate your overall experience with the 2017 summit?", 30 respondents answered that the quality of the summit was Excellent (highest rating) and 15 answered Good (2nd highest rating).

Table 3 (continued). CTSC activity goals and achieved metrics.

Activity	Measurement Technique	Goals	Achieved
Software Assurance	Post-engagement assurance tool usage by projects, on 3, 6 and 12 month time scale	Linear progression each year on tool use.	Nothing to report yet.
	Number of projects that engage us for the Moderate and Deep Dive levels.	3-4 requests for engagements each year.	In our two engagement application cycles in 2017, eight applicants requested code reviews.
	Number of groups using online training materials	Linear progression each year.	Nothing to report yet.
Outreach / Community Impact	Presentations at Project/PI Meetings	4-6 per year	On track, and exceeding. Presentations at GPN webinar, CASC, NSF FacSec, SPAN, SAC-PA, NRP, NSF Large Facilities CI workshop, and NSF LF Workshop in 2017. Poster at NSF SI2 PI meeting.
	Mentions in NSF Solicitations	Goal is all solicitations with a requirement for a cybersecurity program to mention us as a resource.	NSF 17-526. None in 3Q2017.
	Webinar attendance and views of archives (new)	Continued growth	Attendance: 333 Archive views: 755
	Subscribers to CTSC email Lists (new)	Continued growth	Announce: 617 (-20 since Q3) Discuss: 328 (+7 since Q3)
	Large facilities participating in Large Facilities Security Team (new)	Goal is to have all Large Facilities participating.	22/25 participating

7 List of All CTSC Engagements

Table 4. All CTSC Engagements (in progress and completed) under current award

Engaged Project	NSF Award # or Category	Engagement Subject
Array of Things	1532133	Assisting in crafting a privacy policy and reviewed cybersecurity program
Cal Poly Pomona SFS	1504526	Assist the Cal Poly Pomona Scholarship for Service Program in providing SFS students experience and training in securing cyberinfrastructure. Provide mentoring to CPP on developing campus cyberinfrastructure, including developing cybersecurity plans.
Cloud Security Best Practices: Agave Platform, Cornell University Center for Advanced Computing, CyVerse, Jetstream (1H2018)	1450437, 1541215, 0735191, 1265383 and, 1445604	Develop cybersecurity best practices for cloud operators.
Design Safe	NHERI: CI-1520817	Cybersecurity review of Design Safe's CI.
DKIST Data Center	AST-0946422	Assisting in the development of an information security program and providing training for staff.
Gemini Observatory	Large Facility	Reviewing and updating core policy processes and documentation, as well as a close unified look at ICS/SCADA, technical, and physical controls at Gemini North
Gen App (1H2018)	1740097	Assisting in developing information security program. In collaboration with SGCI.
HUBzero (2016)	Used by multiple NSF projects.	Assisting in writing a Master Information Security Policy and Procedures document to lay out the project's overall strategy, roles, and responsibilities
LIGO (2016)	Large Facility	Assisted in search for CISO.
NRAO (1H2018)	1647378	Evaluation of existing information security program.

Table 4 (continued). All CTSC Engagements (in progress and completed) under current award

Engaged Project	NSF Award # or Category	Engagement Subject
Multi-Institutional Open Storage Research Infrastructure (MI_OSiRIS)	1541335	Federated identity and access management.
Open Science Grid/HTCondor-CE	1148698	Cybersecurity review of HTCondor-CE
University of New Hampshire Research Computing Center	1541430	Assistance in developing an information security program. Quick evaluation of information security program with recommendations for improvement. Training for staff.
SciGaP	1339774	Assisted with the design of security and identity management functionality of services that support science gateways
TransPAC	1450904	Supporting development of cybersecurity program.
United States Antarctic Program	Operated by National Science Foundation's Office of Polar Programs	Reviewed processes and policies relevant to polar science information security.
Wildbook/IBEIS	1550881	Collaborated on the development of a role-based access control (RBAC) prototype for the next generation Wildbook platform.

Table 5. CTSC Engagements under prior award (1234408)

Engaged Project	NSF Award # or Category	Engagement Subject
perfSONAR	Extensively used by R&E community and numerous CC-NIE awardees	Reviewed vulnerability management practices and performed code review of bandwidth controller (BWCTL)
AARC	EU Project	Collaborated to gather input from US cyberinfrastructure projects on AARClead activities, disseminate training and other AARC project outputs to US cyberinfrastructure projects, and facilitate EUUS pilot project activities.
HUBzero (2014-15)	Used by multiple NSF projects.	Review of Web Server Security Model and Disaster Recovery Plan documents.
OOI	Large Facility	Assisted in developing cybersecurity program.
LSST	Large Facility	Assisted in developing cybersecurity program.
NEON	Large Facility	Performed cybersecurity risk assessment on the NEON network of sensors and data servers.
CC-NIE (U. Cincinnati & U. Pittsburgh)	1440646 and 1541410	Facilitated peer-to-peer review of cybersecurity programs.
CC-NIE (U. Oklahoma)	1341028	Cybersecurity program review and guidance. Determined engagement was too early and suspended.
NTP	Core Internet infrastructure	Assisted in migration of source code to open source repository, modernization of build and test infrastructure, creating documentation suitable for onboarding new developers, and pruning old code.
DKIST	Large Facility	Assisted in development of a cybersecurity program. Cybersecurity Program Guide was key output.
Globus	Used by many NSF projects.	Conducted cybersecurity review of the architecture and design of the new sharing functionality.

Table 5 (continued). CTSC Engagements under prior award (1234408)

CC-NIE (Penn State and U. Utah)	1245980 and 1341034	Facilitated peer-to-peer review of cybersecurity programs.
LTER Network Office	0832652	Assisted in developing a risk-based cybersecurity plan.
LIGO (2013)	Large Facility	Assisted in supporting international identity federation.
DataONE	1430508	Design-level review of the DataONE IdM system implementation.
Pegasus	Multiple	Reviewed practice of securely supporting data staging.
IceCube	Large Facility	Assisted in developing a cybersecurity plan.
CyberGIS	1047916	Performed risk assessment of the CyberGIS Gateway system architecture.