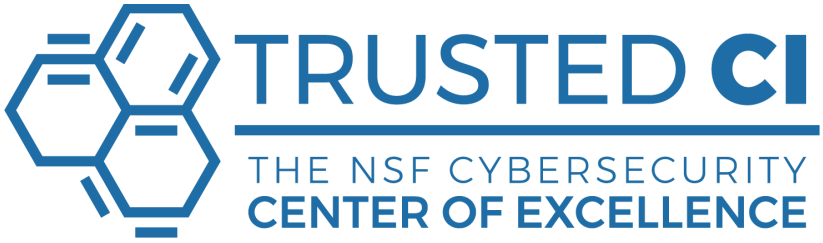

Annual Report for 2018 / Project Year Three

Trusted CI
The NSF Cybersecurity Center of Excellence

NSF Grant ACI-1547272

January 1, 2018 - December 31, 2018

For Public Distribution

Trusted CI Team

Andrew Adams[1], Kay Avila[3], Joel Atkins[4], Jim Basney[3] (co-PI), Leslee Bohland[2], Diana Borecky[2], Robert Cowles[5], Jeannette Dopheide[3], Terry Fleury[3], Grayson Harbour[2], Dr. Elisa Heymann[4], Florence Hudson[5], Craig Jackson[2] (co-PI), Ryan Kiser[2], Mark Krenz[2], Jim Marsteller[1] (co-PI), Prof. Barton Miller[4] (co-PI), Warren Raquel[3], Preston Ruff[2], Scott Russell[2], Zalak Shah[2], Anurag Shankar[2], Susan Sons[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 Trusted CI

Trusted CI 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. Trusted CI 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 Trusted CI, 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.

Using & Citing this Work

Please cite this work as:

> Trusted CI Annual Report for 2018. December, 2018. http://hdl.handle.net/2022/22597

For updates to this report and other reports from Trusted CI, please visit https://trustedci.org/reports/

Trusted CI 2018 Highlights

A. The 2018 NSF Cybersecurity Summit was executed by Trusted CI August 21-23 in Alexandria, VA. The attendance was 117 people at the plenary, and 95 people, a new high,attended the opening training and workshop day.

B. Trusted CI's supplemental proposal to NSF was funded, continuing Trusted CI's activities through 2019 and expands our scope to add a Fellows Program (led by Dana Brunson at Oklahoma State), an effort to Transition Cybersecurity Research to Practice (led by Florence Hudson), and undertake an updated expansion to the OSCRP as part of the Trusted CI Cybersecurity Program Framework. Florence Hudson joined Trusted CI in 3Q2018 to begin work on the transition of cybersecurity research.

C. Trusted CI completed its rebranding from CTSC.

D. Trusted CI's work was prominently and positively mentioned numerous times by the community, including NSF's Cybersecurity Innovation for Cyberinfrastructure solicitations (18-547 and 19-514), on the NSF Large Facilities Office website, by the director of the NSF Office of Advanced Cyberinfrastructure in a public talk, and in the NSF Large Facilities Cyberinfrastructure Workshop report.

E. The Trusted CI webinar series hosted ten talks with 299 total attendees and over 600 views of recordings. The August talk, "NIST 800-171 Compliance at University of Connecticut" with Jason Pufahl, saw 111 non-Trusted CI live attendees, our highest attended webinar to date.

F. We held two calls for engagement applications, receiving 10 total applications and accepting 8. We completed engagements with NRAO, HTCondor/OSG, GenAPP, the Environmental Data Initiative, Open OnDemand, and SI2-SSI: SAGE2, GISandbox, and the 'Ike Wai project at the University of Hawaii (the latter two through our collaboration with the Science Gateway Community Institute). We have four engagements scheduled for the first part of 2019: the Polar Geospatial Center, the American Museum of Natural History, the Singularity Project, and Purdue University.

G. In addition to the individual engagements, in collaboration with the Agave Platform, the Cornell University Center for Advanced Computing, CyVerse , and Jetstream, we produced a publication on Cloud Security Best Practices, and disseminating that via presentations at the NSF Cybersecurity Summit and a Trusted CI webinar.

H. Following up with previous engagements and asking "How likely are you to recommend that other researchers, projects, or facilities engage with Trusted CI?" resulted in 21 of

23 responding 5 out of 5 (“Extremely likely”) and the other two responding 4 out of 5 (“Very Likely”) .

I. Our Cyberinfrastructure Vulnerabilities program issued 15 cyberinfrastructure vulnerability alerts to 108 subscribers.

J. Software security materials developed by Trusted CI, and freely available online, were used in a course at University of Wisconsin, delivered to 20 students.

K. Six publications were produced: The Trusted CI Vision for an NSF Cybersecurity Ecosystem And Five-year Strategic Plan (2019-2023), the Report of the 2017 NSF Cybersecurity Summit, 2017 NSF Community Cybersecurity Benchmarking Survey Report, the Trusted CI Broader Impacts Project Report, Security Best Practices for Academic Cloud Service Providers, and the Report of the 2018 NSF Cybersecurity Summit.

L. Presentations and trainings were delivered at EDUCAUSE Security Professional Conference, Internet2 Global Summit, the Strategic Partnership for Advanced Cyber Infrastructure @ Minority Serving Institutions workshop, the NSF SI PI meeting, the SGCI Bootcamp, the Indiana University Statewide IT Conference, the NSF OAC Webinar, the NSF Cybersecurity Summit, PEARC18, the Science Gateways Community Institute webinar, the U.S. European Command JCC International Cyber Summit, and KINBERCON.

M. Craig Jackson is PI of a new Department of Defense-funded cybersecurity assessment project, leveraging experience from Trusted CI. While he will remain involved in Trusted CI, he will be stepping down as Trusted CI co-PI.

N. In an effort to improve coordination across CI Projects, cybersecurity leaders from XSEDE, OSG and Trusted CI held a meeting at the NSF Cybersecurity Summit to discuss current and planned activities and determine where collaboration would be of value.

O. PI Welch’s proposal to establish the ResearchSOC, a collaborative security response center under CICI 18-547, was funded and he, along with co-PI Marsteller, have begun coordination between these two NSF cybersecurity centers while ensuring no conflicts of interest arise.

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 2018 NSF Cybersecurity Summit[1] was executed by Trusted CI August 21-23 in Alexandria, VA. The summit was built on the success, findings, and lessons learned from previous years. The attendance of 117 people at the 2018 Summit was roughly unchanged from last year's summit, although this year there were 60 new attendees who had not attended the 2017 summit. There were 95 individuals attending the training and workshop day this year, an increase from 83 in 2017, 75 in 2016 and 45 in 2015.

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. The Summit's 117 attendees represented 55 NSF projects (89 of the attendees are affiliated with an NSF award), and a total of 21 large facilities were represented.

Keynote speakers included Amy Friedlander (NSF) Deputy Office Director of the Division of OAC, and Von Welch, director of the Indiana University Center for Applied Cybersecurity Research and PI for Trusted CI. The location of the 2018 summit followed the NSF's office move to Alexandria, VA. Early on in the planning process it was determined that a move to a venue in Alexandria would involve added cost at the new venue site that was not accounted for in the initial grant funding, thus Trusted CI addressed the issue by implementing a modest fee of $200 to attend the summit. Moreover, this was the first year we implemented a Code of Conduct in order to be proactive about potential issues at the summit and help make all attendees feel welcome and safe at the summit.

Feedback for the summit and training sessions is very positive with 98% reporting the summit experience as "Excellent/Good."

In PI Von Welch's talk at the summit[2], which he unofficially titled *Cybersecurity: We don't have it right yet*, he put forth the insight that security suffers from an inability to demonstrate its value, as well as presenting the notion that cybersecurity must keep a broad focus on all IT risks, not just those responsible due to malicious actors. He further explored the idea of re-examining the CIA triad (i.e., confidentiality, integrity and availability) for science and research, suggesting that

[1] https://trustedci.org/2018-nsf-cybersecurity-summit/
[2] https://doi.org/10.6084/m9.figshare.7011785

efficient (available, collaborative and fast), trusted (integrity, quality assured and defensible) and reproducible reflect better the goals of science.

Training presented by Trusted CI and others responding to our call for particulation at the Summit included:

- Industrial Control System Security - Existing Infrastructure and New Designs, Phil Salkie. https://iu.app.box.com/s/g2y4notvxoh5mgalnkh5o79vjfe58bt6/folder/52716421803
- Setting up a compliance program for CUI, Erik Deumens. https://iu.app.box.com/s/g2y4notvxoh5mgalnkh5o79vjfe58bt6/folder/52717550601
- Automated Assessment Tools - Theory & Practice, Barton P. Miller and Elisa Heymann. https://iu.app.box.com/s/g2y4notvxoh5mgalnkh5o79vjfe58bt6/folder/52717593017
- Developing Cybersecurity Programs for NSF Projects, Kay Avila, Bob Cowles and Craig Jackson. https://iu.app.box.com/s/g2y4notvxoh5mgalnkh5o79vjfe58bt6/folder/52717244928
- Software Engineering Guide for NSF Science, Susan Sons. https://iu.app.box.com/s/g2y4notvxoh5mgalnkh5o79vjfe58bt6/folder/52715678700
- Compliance 101: HIPAA, FISMA, NIST 800-171 and GDPR, Anurag Shankar, Susan Ramsey and Scott Russell. https://iu.app.box.com/s/g2y4notvxoh5mgalnkh5o79vjfe58bt6/folder/52716843381
- Security Log Analysis, Mark Krenz. https://iu.app.box.com/s/emma9tr2xb5w6jyfbbiwgpogyel63sb6
- WISE Workshop, David Kelsey, Romain Wartel, David Crooks, Adam Slagell, Uros Stevanovic and Ralph Niederberger. https://iu.app.box.com/s/0g7dqf65hjf142mi8lqjkjr2asm1vx49

This year we continued to encourage and host international participation with the inclusion of the WISE (Wise Information Security for collaborating 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, EOSC-hub, 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
- Operational Security threat intelligence and communication between SOCs
- SCI working group including a Policy Development Kit, Acceptable Use Policies and discussion of the risks to Cyberinfrastructures resulting from Data Privacy issues and the new European Union General Data Protection Regulation (GDPR).
- Security challenges for high-throughput data transfers

The WISE workshop hosted at the summit enabled the collaboration and exchange of operational practices between US and European based Cyberinfrastructure communities.[3]

This year the summit's attendance dropped slightly to 117 compared with 120 in 2017, however, just over half of the attendees at the 2018 summit had not attended the 2017 summit. We performed a survey following the summit among people who had attended the previous year's summit, but not the 2018 summit. Of the 21 responses, we found that the vast majority of reasons were not related to the quality of previous summit events. Most cited funding issues or scheduling conflicts as being the reason for not attending. None of the responses indicated that the $200 fee was an issue.

A more comprehensive report of summit activities and outcomes has been published[4].

Plans for next year: Plan and execute the 2019 summit slated for October 2019 in San Diego.

1.2 Large Facility (LF) Outreach

Co-PI James Marsteller attended the NSF Large Facilities Workshop April 30th-May 2nd in Washington D.C. as a Trusted CI Liaison. The workshop provided an opportunity to learn about the operational aspects of large facilities including development, planning and construction. Of particular interest was a session delivered by Rebecca Yasky on Knowledge Management for improving communication among facilities and NSF. Different techniques were explored to determine which work best to facilitate communication, for example sharing lessons learned through group discussion. Marsteller shared examples of successful communication tools used by Trusted CI for the Large Facilities Security Team (LFST) and CI Vulnerability program. We were very happy to learn that the Large Facilities Office recently updated their public website with a list of resources that includes a link to the Trusted CI Blog highlighting the "Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects".[5] Additionally, Trusted CI's presentations at the NSF Large Facilities Workshops appear in the NSF Major Facilities Knowledge Sharing Gateway[6].

The LFST has continued to meet on a monthly basis, featuring a topic of interest relating to cybersecurity. For example in March the group discussed the policy lifecycle; getting the support from senior management and strategies for policy implementation & compliance. Timely operational security discussions such as the impact and response by LFs to the Meltdown/Spectre vulnerability and the EU GDPR were also featured. Some of the LFST attended the 2018 NSF Cybersecurity Summit. During the first day of plenary at the summit the

[3] https://wiki.geant.org/display/WISE/WISE+@+NSF+CyberSecurity+Summit+2018
[4] http://hdl.handle.net/2022/22588
[5] https://www.nsf.gov/bfa/lfo/
[6] https://www.largefacilitiesworkshop.com/knowledge-gateway/

LFST had an informal meeting over lunch. The lunch meeting is one of the few events at which team members have an opportunity to meet in person.

Finally, the report from the 2017 NSF Large Facilities Cyberinfrastructure Workshop[7], published in 2018, mentioned Trusted CI (as its name at that time: "CTSC") as a model to follow for future centers.

Plans for next year: Trusted CI will continue ongoing coordination of the LFST along with ongoing development of the NSF Large Facilities Manual[8] subsection of Cybersecurity. We also plan on releasing a new, updated version of the guide for developing cybersecurity programs for NSF projects as the Trusted CI Framework: An Architecture for Cybersecurity Programs.

Fig 1. LFST Group Photo from NSF Cybersecurity Summit 8/22/18

Support for the Large Facilities Manual (LFM) continued in 2018. The NSF provided feedback on the draft cybersecurity subsection of the Large Facilities manual during the third quarter. The latest comments were provided by the CISE Major Facilities Working Group. The revision was a substantial shortening of the previous version. Trusted CI responded to the revised draft and are awaiting for the LFM to be open for public review in December 2018.

[7] http://facilitiesci.org/
[8] https://www.nsf.gov/bfa/lfo/lfo_documents.jsp

1.3 Webinar Series

The monthly CCoE Webinar Series (https://trustedci.org/webinars/) continued through 2018. Table 1 shows the number of webinar attendees and archive viewers in 2018.

Table 1. Trusted CI Webinar attendance and archive viewing.

Date	Topic	Speaker(s)	Attended[9]	Watched Later[10]
Feb.[11]	SMARTDATA Blockchain	Murat Kantarcioglu	21	64
Mar.	Data Quality & Security Evaluation Framework Dev.	Reznik & Khokhlov	14	94
April	Toward Security-Managed Virtual Science Networks	Jeff Chase & Paul Ruth	22	39
May	EU's GDPR	Scott Russell	39	163
June	Security Program at LSST	Alex Withers	30	42
July	Trustworthy Computing for Scientific Workflows	Mayank Varia & Andrei Lapets	12	70
Aug.	NIST 800-171 Compliance at University of Connecticut	Jason Pufahl	111	109
Sept.	SCI Trust Framework	David Kelsey	21	27
Oct.	Urgent Problems and (Mostly) Open Source Solutions	Jeff Spies	13	29
Dec.[12]	Best Practices for Academic Cloud Service Providers	Rion Dooley	16	No data yet
Total			**299**	**637**

A couple of presentations in 2018 stood out in attendance and content. The May webinar, presented by Trusted CI's Scott Russell, was an overview of the EU's GDPR and its potential impact on the NSF community. It was a very successful presentation and has become one of the more popular webinars on our YouTube channel. One of the survey respondents wrote,

> "Thank you! I've attended several webinars and meetings on GDPR. Very clear and clarifying even. Peeling away the layers of the onion... very well. It might be nice to

[9] Does not include Trusted CI staff and presenters.
[10] Either On-demand or on YouTube
[11] January's webinar was cancelled due to speaker illness. The first webinar in 2018 was in February.
[12] Due to frequent travel during November and December, we do not present a webinar in November and instead schedule it in mid-December before the holidays.

have a repeat of this webinar in 6 months or 1 year, once there is some relevant case law or other guidance published. Thanks again."

The August talk, “NIST 800-171 Compliance at University of Connecticut” with Jason Pufahl, saw 111 non-Trusted CI live attendees, our highest attended webinar to date. We attribute some of the high attendance to EDUCAUSE sharing the event on their security list. Our relationship with EDUCAUSE has helped amplify some of the work we are doing.

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 2018 the videos from our series received approximately 908 views, this number includes views of presentations recorded prior to 2018.

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 2018 we’ve added 85 subscribers to “announcements” and 87 to “discuss.”

To schedule the webinar series we first reach out to active CICI award recipients and offer an opportunity to present. The awardees end up giving the largest share of the presentations during the year. This targeted outreach strategy has the added benefit of Trusted CI helping promote the NSF CICI program. In 2018 we presented 4 CICI projects. In 2019 we have scheduled at least 7 CICI awardee projects.

Plans for next year: We have booked the following presenters in 2019 so far:

- **January:** The Research Security Operations Center (ResearchSOC)
- **March:** SecureCloud
- **April:** Supporting Controlled Unclassified Information with a Campus Awareness and Risk Management Framework
- **May:** Robust and Secure Internet Infrastructure for Scientific Collaboration
- **June:** The Trusted CI Framework: An Architecture for Cybersecurity Programs
- **July:** Campus Infrastructure for Microscale, Privacy-Conscious, Data-Driven Planning
- **August:** Pegasus and IRIS
- **December:** The DDoS Defense In Depth for DNS (DDIDD) Project

1.4 Science Gateways Community Institute Partnership

We continue to partner with the Science Gateways Community Institute (SGCI, NSF award #1547611 and one of the two initial NSF SI2 institutes) to collaboratively fund half of a security analyst focusing on security for science gateways. Trusted CI participated in SGCI’s May and August bootcamps in Austin, TX and Chicago, IL, respectively, presenting *Cybersecurity For*

Gateways.[13] A bootcamp is a week-long intensive program for those who want to further develop and scale their gateways. A key theme is sustainability.[14] Previous cybersecurity presentations by Trusted CI at bootcamps focused more on software security. A change in Trusted CI staff between bootcamps brought new content, which focused more on providing guidance on overall operational cybersecurity best practices and resources for further guidance. Moreover, we attended as both a sponsor and exhibitor at SGCI's Gateways '18 Resource Expo.[15]

Trusted CI additionally performed a scan of SGCI documents stored in the cloud to check their permissions and provided a report of all document permissions, highlighting those that had open permissions that could potentially be viewed by unauthorized individuals. In the process, an exposed document was discovered that contained sensitive operational information. Trusted CI worked with SGCI to correct the exposed information, as well as provided advice on how to protect and manage permissions on all documents stored in the cloud. Furthermore, SGCI expressed interest in utilizing and further developing the "cloudperm" software created by Trusted CI staff to perform the scan, and have agreed that a portion of Trusted CI's contribution to SGCI would go to extend the reporting functionality of the cloudperm software.

Through SGCI's Incubator project, Trusted CI engaged with two gateway projects in the past year, GISandbox and Ike Wai (NSF award #1557349), to perform security assessments of their gateways.[16] The assessment of the GISandbox project gateway focused on two aspects of their overall security: a review of their system's operational security, and a security review of their science gateway program code. The Ike Wai project's gateway involved a review of their identity and access management (IAM) implementation, as well as providing a security program. Both gateway assessments were completed.

Finally, Sean Cleveland, the lead software architect at the University of Hawai'i's (UH) `Ike Wai gateway, expressed the need for security in their project and specifically cited Trusted CI as a valued collaborator.[17]

Plans for next year:

- **Q1-4:** Provide cybersecurity consultation to new SGCI Incubator clients.
- **Q2**: Provide cybersecurity training at upcoming SGCI bootcamp at Indianapolis, IN in May.
- **Q3**: Provide cybersecurity training at second SGCI bootcamp in 2019, location yet unspecified.

[13] http://hdl.handle.net/2142/100440
[14] https://sciencegateways.org/engage/bootcamp
[15] https://sciencegateways.org/web/gateways2018
[16] https://sciencegateways.org/consulting
[17] https://sciencenode.org/feature/Hawaii%20H2O.php

1.5 Trusted CI at PEARC

Trusted CI had an expanded role at PEARC18 this past year in Pittsburgh, July 22-26.[18] Craig Jackson and Bob Cowles presented the workshop "Practical Cybersecurity Programs for Science Projects and Facilities."[19] It covered practical information security for science projects by describing the foundational elements of a cybersecurity program necessary to provide a secure and safe environment for science. The emphasis of their workshop was on the four pillars of such a program: Alignment to Mission - identification of critical resources and processes; Resources - money, people; Governance - roles and responsibilities, risk management and acceptance, policies; Controls - selecting a good baseline control set, and included guidance on maintaining and evaluating an established cybersecurity program. Additionally, Susan Sons offered the workshop "Software Engineering Practice for Science, Research, and Scientific CI."[20] Her presentation introduced the Software Engineering Guide under development at Trusted CI, which provides guidance and tools for building security into the development, packaging, distribution, and management of software in support of science and research.

Von Welch also acted as moderator to a question and answer session with Anita Nikolich following her presentation "Hacking Academia," a talk which explored the utility in connecting the academic community, cybersecurity operators and non-academic security researchers.[21]

Trusted CI further increased their visibility by becoming an exhibitor through PEARC's sponsorship program (with non-NSF funds).[22] Our exhibitor's table was well-received at the conference with copies of a number of our best practices distributed.

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 PEARC'19 (in Chicago, IL) has been released[23] and we plan similar contributions and interactions.

[18] https://www.pearc18.pearc.org/
[19] https://pearc18.conference-program.com/?page_id=10&id=work112&sess=sess126
[20] https://pearc18.conference-program.com/?page_id=10&id=specmeet104&sess=sess190
[21] https://pearc18.conference-program.com/?page_id=10&id=plen106&sess=sess146
[22] https://www.pearc18.pearc.org/exhibitor-prospectus
[23] https://www.pearc19.pearc.org/call-for-participation

Fig 2. Trusted CI's Exhibitors Booth at PEARC18

1.6 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 NSF science community, Trusted CI, and other stakeholders with a baseline view of the state of the community, and facilitate an understanding of changes over time. In 2017 we continued and expanded this survey, refining the questions based on the analysis of the 2016 report.[24]

Preliminary findings for the 2017 Survey Report were circulated in March 2018 within Trusted CI, and the final Survey Report was published in June 2018.[25]

The 2017 Survey was notable for the particularly high response rate of NSF Large Facilities, increasing from 9 (out of 27 responses) in 2016 to 15 (out of 20 responses) in 2017. Other noteworthy findings include: 10 out of 20 respondents utilize the Trusted CI Guide as a governing cybersecurity framework, including 9 Large Facilities; cybersecurity budgets, best practices, concerns, and trajectories all vary greatly, without any clear relationship to overall size or budget; and multi-factor authentication adoption increased from 6 (out of 27) in 2016 to 12 (out of 20) in 2017.

[24] http://blog.trustedci.org/2016/06/help-ctsc-build-our-community.html
[25] Russell, Jackson, & Cowles. "2017 NSF Community Cybersecurity Benchmarking Survey Report," (8 June 2018), https://scholarworks.iu.edu/dspace/bitstream/handle/2022/22171/2017%20Community%20Survey%20Report.pdf?sequence=2&isAllowed=y.

In September, we developed the Community Survey Strategic Plan, where we outlined a set of options for the Community Survey in future years. The Strategic Plan and the options contained therein were circulated within the Trusted CI team. The team agreed to shift the Survey to a 2 year cycle, circulating the Survey in the Spring and the Report in the Fall, and focusing the Survey on Large Facilities and other large science projects.

Finally, in November, we circulated a request for suggested additions, modifications, or deletions to the Community Survey questionnaire.

Plans for next year: We will circulate the 2019 Survey Questionnaire and publish a report analyzing the data collected therein.

1.7 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 described elsewhere at PEARC and the NSF Cybersecurity Summit). A list of presentations and slides presented may be found at https://trustedci.org/presentations/

- Anurag Shankar. Securing Research Data on Campus – Not Just HIPAA and FISMA, Indiana University Statewide IT Conference October 2018.
- Mark Krenz. Your Cloud Data Exposed, a look at the issues of sharing documents on Google Drive and Box, Indiana University Statewide IT Conference October 2018.
- Von Welch. *Cybersecurity to Enable Science: Hindsight and Vision from the NSF Cybersecurity Center of Excellence*. NSF OAC webinar, September 2018.
- Von Welch. *Cybersecurity: We Don't Have It Right Yet*. 2018 NSF Cybersecurity Summit Keynote, August 2018.
- Grayson Harbour. *Evidence Based Cybersecurity.* 2018 NSF Cybersecurity Summit Presentation, 23 August 2018.
- Jim Basney, August SGCI Bootcamp. Cybersecurity for Gateways.
- Anita Nikolich, Von Welch. Trusted CI Panel Presentation at PEARC18, July 2018.
- Von Welch. Cybersecurity for Research on Small Campuses. Strategic Partnership for Advanced Cyber Infrastructure @ Minority Serving Institutions, June 2018.
- Anurag Shankar and Jim Basney presented "Cybersecurity for Research on Campus: Not Just HIPAA & FISMA" at the Internet2 Global Summit, May 2018.
- Warren Raquel led a pre-conference workshop, "Incident Response Training", at the EDUCAUSE Security Professionals conference, April 2018.
- Mark Krenz led a pre-conference workshop, "Security Log Analysis", at the EDUCAUSE Security Professionals conference, April 2018.

- Anurag Shankar, Jim Basney, and Von Welch presented "Cybersecurity for Research on Campus: Not Just HIPAA & FISMA" at the EDUCAUSE Security Professionals conference, April 2018.
- Von Welch and Mark Krenz presented “Cybersecurity for the Modern Science Gateway” at the Science Gateways Community Institute webinar, February 2018.
- Bart Miller and Elisa Heymann gave a talk on “Cyber-Security of Maritime Container Terminals” at the U.S. European Command (USEUCOM) JCC International Cyber Summit in Garmisch, Germany, March 2018.

Fig 3. Photo from the USEUCOM International Cyber Summit.

Plans for next year: For 2019, our presentation plans include the following:

1. Invited talk at the Society of Industrial and Applied Mathematics (SIAM) 2019 Computational Science and Engineering (CSE19) conference Broader Engagement (BE)[26]
2. CENIC 2019 Annual Meeting[27] (submitted and pending acceptance)
3. Internet2 Global Summit[28]
4. Invited talk at the International Symposium on Grids and Clouds (ISGC) 2019[29]
5. 2019 EDUCAUSE Security Professionals Conference[30] (submitted and pending acceptance)

[26] http://shinstitute.org/siam-cse19-be-program/
[27] https://events.cenic.org/march-2019
[28] https://meetings.internet2.edu/2019-global-summit/
[29] http://event.twgrid.org/isgc2019/
[30] https://events.educause.edu/security-professionals-conference/2019

6. PEARC19[31] (submission planned)

1.8 Cybersecurity Research Transition to Practice

Transition To Practice (TTP) is critical to bring the value of government investment in successful cybersecurity research to the operational world to make cyberspace safer. We have incorporated Cybersecurity Research TTP into the CCoE, as it supports our mission to mature the NSF Cybersecurity Ecosystem by filling in gaps in current capabilities, while leveraging our deep connections in higher education information security, NSF CI cybersecurity, and NSF cybersecurity research communities. We added Florence Hudson to the Trusted CI team to lead the TTP effort beginning in July 2018. Florence developed and executed a Cybersecurity TTP program as Chief Innovation Officer at Internet2 as PI for EAGER #1650445.

Successful TTP can be via commercialization, industry partnerships, start-ups, open source, or deployment in higher ed, NSF projects, or government. Hence, in 2H18 we decided to begin by interviewing cyber-infrastructure and cybersecurity experts from higher ed, industry, and NSF projects to identify cybersecurity needs and gaps which we might fill with cybersecurity research. The top cybersecurity needs / gaps identified are:

- Leverage of Artificial Intelligence / Machine Learning for cybersecurity, including log analysis, intrusion detection, insider/outsider threat, data reduction, SW verification
- Global distributed federated identity management - students, researchers, patients, devices, clients, employees – to ease collaboration and reduce risk
- Tools for Internet of Things (IoT) device discovery, then to assess and reduce IoT privacy and security risk
- Security and privacy education and workforce development, including hands-on experience for developers, awareness for end users and decision makers

The Top TTP needs / gaps identified were:

- Include business partners with the researchers and practitioners in the TTP matchmaking, e.g., entrepreneurs, industry, VC's, angels, to enable collaboration
- Add "Co-creation" to the TTP workshop to clarify needs, research fit-for-purpose, and develop steps to transition research to operational practice
- Enable earlier collaboration between researchers and practitioners so software and solutions are developed with operations in mind
- Provide testbeds to test research before deployment (perhaps leverage DETER@ISI/USC, Research SOC)

We are analyzing NSF awards to identify research/researchers to fill the cybersecurity gaps, and then enable matchmaking between the practitioners who identified the cybersecurity gaps and

[31] https://www.pearc19.pearc.org/

the researchers and research in order to enable cybersecurity research transition to practice. This analysis includes 903 SaTC awards from 2011 through 2019, 99 TTP awards from 2014 through 2018, and CICI PI quad chart presentations from the 2017 and 2018 CICI PI meetings. , As we build a collaborative cybersecurity research and practitioner community, preliminary work has resulted in some one-on-one matchmaking between NSF researchers and practitioners. As we plan for the 2019 cybersecurity TTP workshops, we will continue one-on-one matchmaking with industry and higher ed practitioners to collaborate with cybersecurity researchers to pilot and transition cybersecurity research to practice.

Plans for next year: The cybersecurity research TTP actions we are planning for 2019 include:

- Enable collaboration and matchmaking between practitioners and researchers to fill cybersecurity gaps, begin with 1:1 discussions, leading up to a workshop, and beyond
- Plan and execute 2019 cybersecurity research TTP and co-creation workshop, including industry and higher ed practitioners, researchers, business partners
- Present at the 2019 EDUCAUSE Security Professionals Conference with co-presenters Helen Patton, The Ohio State University CISO, and Ed Aractingi, Marshall University CIO (session proposal entitled “Transitioning Cybersecurity Research to Practice to Solve Cybersecurity Challenges” submitted and pending acceptance)
- Continue collaboration with Alec Yasinsac, University of South Alabama, with possibility of leveraging the TTP mentors developed from his NSF TTP grant to enable matchmaking
- Invite cybersecurity researchers to present at TrustedCI webinars

1.9 Social Media Impact

This section covers our social media impact, broken down by Twitter impressions[32], blog page views, and unique website visits. Table 2 shows the stats collected in 2018.

[32] Number of times users saw a Tweet on Twitter

Table 2. Social media impact.

Date	Twitter Impressions	Blog Page Views	Website Visits
Jan.	4.5K	1,260	310
Feb.	4.4K	1,678	360
Mar.	3.6K	1,447	354
Apr.	6.7K	1,446	571
May	3.8K	1,491	938
June	7.3K	1,671	912
July	7.5K	2,171	984
Aug.	25.3K	1,874	1,495
Sept.	9.4K	1,382	635
Oct.	6K	2,005	616
Nov.	3.9K	2,049	516
Dec.	No data yet	No data yet	No data yet
Total	**82.4K**	**18.5K**	**7.7K**

1.10 Coordinating Security Across Trusted CI, OSG, XSEDE

In an effort to improve coordination across CI Projects, cybersecurity leaders from XSEDE, OSG and Trusted CI held a meeting at the NSF Cybersecurity Summit to discuss current and planned activities and determine where collaboration would be of value. Two areas were identified: 1) Peer review of XSEDE table top exercises with future active participation between OSG and XSEDE; and 2) Coordination of vulnerability assessments.

To support the latter activity, the lead of the Trusted CI Cyberinfrastructure Vulnerabilities program has joined the XSEDE weekly Incident Response/Trust group meetings. For example CVE-2018-14634, a Linux integer overflow flaw was discussed on the October 1st call. This allowed for a collaborative discussion on the assessment of the vulnerability with key security personnel outside of Trusted CI.

Plans for next year: Trusted CI will continue participating in the weekly XSEDE Incident Response/Trust Group calls. The XSEDE table top exercises are expected to be executed in Q1 of 2019. XSEDE will share the results of the exercise with OSG and Trusted CI and solicit feedback on the process and lessons learned.

1.11 Trustworthy Campus Cyberinfrastructure Workshop

In collaboration with Internet2, and under funding from their grant #1650445, Trusted CI organized the "Enabling Trustworthy Campus CI for Science" workshop[33], held on September 24th and co-located with the NSF CICI/CC-* PI meeting. Thirty members of the community representing 16 institutions attended, including 12 members of the research computing community, 12 chief information security officers or security engineers, 5 VPs of IT or CIOs, and one Dean.

The workshop format was a lightning talk from each institution describing relationships between research computing and information security at their institution, with copious discussion between presentations. The day concluded with breakout sessions exploring commonalities, differences, and lessons learned between and by the institutions. A blog post was made summarizing the workshop results[34].

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[35] 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 Trusted CI 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).

The OSCRP was promoted in NSF's CICI solicitations (18-547[36] and 19-514[37]) as a suggested tool for applicants in two of the three areas of the solicitation.

Plans for next year: We will extend the OSCRP with additional science assets, in particular, sensor networks and control systems, and incorporate it into our Trusted CI Framework (see Section 2.6).

[33] https://www.thequilt.net/public-event/internet2-eager-grant-workshop/
[34] https://www.internet2.edu/blogs/detail/16960
[35] https://scholarworks.iu.edu/dspace/handle/2022/21259
[36] https://www.nsf.gov/publications/pub_summ.jsp?ods_key=nsf18547
[37] https://www.nsf.gov/pubs/2019/nsf19514/nsf19514.htm

2.2 Situational Awareness / Cyberinfrastructure Vulnerabilities

The Cyberinfrastructure Vulnerabilities team provides concise announcements on critical vulnerabilities that affect science 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 Trusted CI's mailing lists[38].

We monitor a number of sources for software vulnerabilities of interest. For those issues which warrant alerts to the Trusted CI 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 maximize the benefit from community expertise.

Some of the sources we monitor for possible threats to CI include:

- OpenSSL, OpenSSH, and Globus project and security announcements
- US-CERT advisories[39]
- XSEDE announcements
- RHEL/EPEL advisories
- REN-ISAC Alerts and Advisories[40]
- Social media, such as Twitter, and Reddit (/r/netsec and /r/security)
- News sources, such as The Hacker News, Threatpost, The Register, Naked Security, Slashdot, Krebs, SANS Internet Storm Center and Schneier

In 2018, we issued 15 cyberinfrastructure vulnerability alerts to 108 subscribers.[41]

Plans for next year: We will continue to provide the Cyberinfrastructure Vulnerabilities service in collaboration with the ResearchSOC (see Section 5.10).

2.3 Publications

Trusted CI produced the following publications in 2018:

- V. Welch, J. Basney, C. Jackson, J. Marsteller, and B. Miller, "The Trusted CI Vision for an NSF Cybersecurity Ecosystem And Five-year Strategic Plan (2019-2023)," Trusted CI, Apr. 2018 [Online]. Available: http://hdl.handle.net/2022/22178.

[38] See https://trustedci.org/vulnerabilities/
[39] https://www.us-cert.gov/ncas/current-activity
[40] https://www.ren-isac.net/public-resources/AlertsAdvisories.html
[41] https://list.iu.edu/sympa/arc/cv-announce-l

- James Marsteller, Von Welch, Mark Krenz, Andrew Adams, Scott Russell. Report of the 2017 NSF Cybersecurity Summit for Cyberinfrastructure and Large Facilities: Ensuring Data Provenance, Integrity and Resilience. [Online]. Available: http://hdl.handle.net/2022/21882

- S. Russell, C. Jackson, B. Cowles, and K. Avila, "2017 NSF Community Cybersecurity Benchmarking Survey Report," Trusted CI [Online]. Available: http://hdl.handle.net/2022/22171

- J. Dopheide, J. Zage, and J. Basney, "The Trusted CI Broader Impacts Project Report," Trusted CI, 2018 [Online]. Available: http://hdl.handle.net/2022/22148.

- Rion Dooley, Andy Edmonds, David Y. Hancock, Richard Knepper, John Michael Lowe, Edwin Skidmore, Andrew K. Adams, Ryan Kiser, Mark Krenz, Von Welch, "Security Best Practices for Academic Cloud Service Providers." May, 2018. http://hdl.handle.net/2022/22123

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

2.4 Training

Training delivered by Trusted CI in 2018:

- Bart Miller and Elisa Heymann taught a 4-hour tutorial on Secure Coding Practices and Automated Assessment Tools", at the Technical University of Munich, Germany, March 2018.
- Mark Krenz. Security Log Analysis. EDUCAUSE SPC 2018, April 2018.
- Warren Raquel. Security Incident Response. EDUCAUSE SPC 2018, April 2018.
- Mark Krenz. Cybersecurity for the Modern Science Gateway. SGCI Bootcamp, May 2018.
- Craig Jackson, Bob Cowles. "Practical Cybersecurity Programs for Science Projects and Facilities". 2 ½ hours, PEARC'18, Pittsburgh, PA, July 2018.
- Susan Sons. "Software Engineering Practice for Science, Research, and Scientific CI." PEARC'18, Pittsburgh, PA, July 2018.
- Bart Miller and Elisa Heymann presented a half-day tutorial on Automated Assessment Tools – Theory & Practice, at the 2018 NSF Cybersecurity Summit, Alexandria, August 2018. This tutorial included a hands-on part. Hands-on.
- Kay Avila, Bob Cowles, Craig Jackson. "A Practical Cybersecurity Framework for Open Science Projects and Facilities". Half day. 2018 NSF Cybersecurity Summit, Alexandria, VA. August 2018.

Fig 4. Photos from the tutorial at the Technical University of Munich

- Bart Miller and Elisa Heymann presented a half-day tutorial on Secure Coding Practices, Automated Assessment Tools and the SWAMP, a SecDev'18 (IEEE Cybersecurity Development Conference) in Cambridge, MA, September 2018.
- Bart Miller and Elisa Heymann were invited for a presentation and to lead discussions in the Madison chapter of OWASP monthly meeting, in Madison, Wisconsin, October 2018.

Fig 5. Photos from the talk and discussions for the Madison chapter of OWASP.

- Bart Miller and Elisa Heymann taught a half-day tutorial, including a hands-on part on Secure Coding Practices and Automated Assessment Tools at SuperComputing 2018 in Dallas, Texas, in November 2018.

Fig 6. Tutorial at SuperComputing'18 in Dallas.

2.5 Software Security Course Development

As a pilot effort, Bart Miller and Elisa Heymann taught the first offering of a course at the University of Wisconsin-Madison, covering a 1-credit subset of their software security curriculum. This course was based on the video modules and text chapters prepared under the Trusted CI funding.

The course, *CS 638 Secure Programming Techniques,* lasted for four weeks and was taught to 20 students. The class followed the flipped-classroom model where, at home, the students watched the videos modules developed by Miller and Heymann, and read the associated text chapters (material available online[42]).

The class time was used for student interaction, including discussion of the videos and text based on the students' questions, and work on hands-on exercises that reinforced the topic(s) of the day. These exercises were started in class and then finished at home. The self contained hands-on exercises were prepared for Trusted CI, and each exercise was delivered in a virtual machine[43]. In addition, each class session included a quiz to assess the work performed on the hands-on exercises.

The topic covered by CS 638 were:

- Introductory concepts.
- Thinking like an attacker.
- Security problems with Exceptions.
- Security problems with Serialization.
- Security problems with Pointers and Strings.

[42] http://research.cs.wisc.edu/mist/SoftwareSecurityCourse/
[43] research.cs.wisc.edu/mist/SoftwareSecurityCourse/Exercises/security-exercises.ova

- Numeric Errors.
- Injections (Introduction to injections, SQL injections, XML injection, Command injections).
- Web attacks (XSS, CSRF, Session management, OpenRedirect).
- Automated assessment tools and the SWAMP.

The class used their self-contained hands-on exercises for Exceptions, Serialization, SQL Injection, Command Injection, XSS, and CSRF.

The feedback of the students was extremely positive. At the end of the course we received e-mails which included the following comments:

> "This class was wonderful."
>
> "Also kudos for running such an awesome class!"
>
> "I would also like to sincerely thank both of you for giving me an opportunity to be a part of this course. I am a grad student working in the area of machine learning. In this fast-moving field, I write and publish code very frequently. This course has helped me get exposed to the best coding practices. I'm happy that from now on I will be publishing "safer" code to the research community."
>
> "Thank you very much for this wonderful and short semester. I really enjoyed the format of the course and the concepts taught."
>
> "Thank you for teaching this course, I learned valuable information I would never have found without this class."
>
> "The attached file is the last exercise for this course. Thanks again for teaching, and offered such a valuable course as I am thinking of going to a grad school about secure programming!"
>
> "Thank you for the short but engaging semester."

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. Based on the success of this initial course offering, a full 3-credit version of this course is being introduced to be taught at UW-Madison during the Spring 2019 (January 2019) semester, with 120 students enrolled.

As part of our ongoing curriculum development, we have developed more modules and associated text chapters. In particular the new modules are: Introduction and Basic Terminology parts 1, 2, and 3, Thinking Like an Attacker, Directory Traversal, Introduction to Injection Attacks, Command Injections, Code Injections, Introduction to First Principles Vulnerability Assessment,

and Using Tools in the SWAMP. All video modules have captions in English and we are working on captions in Spanish. The videos are available through the Vimeo platform. A prototype for the virtual book, containing all the chapters/modules, in online[44].

We also developed associated hands-on exercises for several of the topics. More specifically we have hands-on exercises for Directory traversal, Exceptions, Command injections, SQL injections, and Web attacks (Cross Site-Scripting and Cross-Site Request Forgery). The exercises are packed in a virtual machine image for VirtualBox , so the students can focus on the security aspects of the exercises in a ready-to-use environment.

Plans for next year: We will teach CS 639 (Introduction to Software Security) at the University of Wisconsin-Madison in Spring 2019. We will also continue developing new modules (both videos and text chapters, with accompanying hands-on exercises). In particular we will focus on attacks for mobile environments.

2.6 The Trusted CI Framework: An Architecture for Cybersecurity Program

Trusted CI's perspective is that the community needs a framework for establishing and maintaining an open science cybersecurity program at any project scale and stage in a project's life cycle. Such a framework would be useful even for projects having significant compliance requirements (e.g., FISMA, HIPAA, NIST SP 800-171) in that it provides a prioritized starting point for evolving a cybersecurity program.

In late 2017, we 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 hoped to substantially improve its scope and quality of content, consistency, and usability for a broad range of NSF projects and facilities.

In 1Q2018, we paused progress on the Guide revision as resources focused on the authors' contributions to the Large Facility Manual subsection on cybersecurity, the Benchmarking Survey, and the NRAO engagement. In 2Q2018, the project team conducted a face-to-face brainstorming, planning and design meeting on May 22-24 in Bloomington, IN for the next Guide version. In Q2/Q3, we substantially revised the Guide-based training to align with our plan to develop and release a new framework. We piloted the training at PEARC'18 and introduced the core concepts of the Framework in a half-day training at the 2018 NSF Cybersecurity Summit. PI Welch featured the Framework in his plenary keynote. On September 27th, we presented the basic architecture and goals of the Framework to the Large Facility Security Team. In 4Q2018, we began broader community engagement including a blog post describing our plans[45] (77 views) and received positive feedback on the Framework's broad

[44] https://research.cs.wisc.edu/mist/SoftwareSecurityCourse/
[45] https://blog.trustedci.org/2018/10/an-open-science-cybersecurity-program_4.html

applicability from other R&D communities (e.g., US Navy), and learned that some community members are already using the Framework (by way of our detailed Summit training materials) to shape their cybersecurity programs. We presented a briefing on the framework at the Fall 2018 HEPiX Workshop in mid-October with 137 registered attendees from 71 countries, and begun coordination with the European effort of WISE SCI on policy templates. As of the end of 2018, we are finalizing major architectural and design decisions.

Plans for next year: In 2019, the Framework is one of our major strategic initiatives. We will complete execution of the first major deliverables, including an implementation guide for scientific CI operators. We will undertake a substantial effort to get community input and buy-in.

2.7 Secure Software Engineering Guide

Funded by a supplement from NSF to bolster Trusted CI software security efforts, we will begin working on a Trusted CI 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 Trusted CI Framework (see Section 2.6), which covers cybersecurity program 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”.

In 2018, we presented the early concepts for the Guide at NSF SI2 PI meeting[46] and material based on this work at PEARC18 and the 2018 NSF Cybersecurity Summit.

Plans for next year: Completion of the guide is behind schedule and was not completed in 2018 as planned. Effort is being allocated in the first half of 2019 to complete the guide with additional oversight by PI Welch.

2.8 Broader Impacts

Examples of Trusted CI’s broader impacts in 2018 are:

- Trusted CI was prominently mentioned as a success in the NSF Large Facilities Cyberinfrastructure Workshop report (http://facilitiesci.org/).

[46] https://si2-pi-community.github.io/2018-meeting/

- The director of the NSF Office of Advanced Cyberinfrastructure referred to Trusted CI as “a very innovative model in providing cybersecurity expertise to NSF large projects such as the NSF Facilities and has been extremely successful."
- The NSF Large Facilities Office featured Trusted CI on their website: https://www.nsf.gov/bfa/lfo/
- Trusted CI sponsored (with non-NSF funds) both PEARC’18 and SGCI’s Research Expo to broaden their audience.
- A security instructor from the FBI’s Enterprise Information Security program reached out to Trusted CI to thank Mark Krenz for making available his presentation slides for security log analysis training from the 2017 GPN AHM presentation. The instructor found the slides helpful in expanding his knowledge. Mark responded with links to updated slides and his BroCon 2017 presentation video.
- In 3Q2018 Von Welch presented, “Cybersecurity to Enable Science: Hindsight & Vision from the NSF Cybersecurity Center of Excellence,” to NSF’s OAC webinar series.
- In 3Q2018 Barton Miller and Elisa Heymann presented, “Critical Infrastructure Software Security: A Maritime Shipping Study,” to the O’Reilly Velocity 2018 conference in London, UK.
- In 4Q2018 Scott Russell presented a modified version of his talk “The European Union General Data Protection Regulation (GDPR)” for the Center of Excellence for Women in Technology (CEWiT) Cybersecurity Camp. (Material originally developed for the Trusted CI Webinar series and updated for the 2018 NSF Cybersecurity Summit.)

Fig 7. Photos from Velocity 2018, in London.

2.9 Trusted CI Broader Impacts Report

In 2018, published the Trusted CI Broader Impacts Report[47]. This report outlines a strategy to help meet the cybersecurity needs of this broader set of NSF projects (both small and large),

[47] https://scholarworks.iu.edu/dspace/handle/2022/22148

and to provide demonstrated value to a significant percentage of NSF projects funded at $1 million or more. The report is broken down into four main sections: quantifying community needs, understanding community needs, evaluating current/potential strategies for broader impacts, and recommending a strategy for broader impacts. The 6 recommended strategies for broadening impacts are:

1. Fill in gaps in our collection of impact statistics (e.g., affiliation of training attendees).
2. Explore outreach opportunities to the Education and Human Resources (EHR) and Biological Sciences (BIO) Directorates, which are currently underrepresented in our impact metrics.
3. Increase attention on developing and maintaining the website, highlighting the content and services we are already providing. Our materials are only as useful as our stakeholders can discover them. It's helpful to consider different stakeholder perspectives when updating and reorganizing the website.
4. Trusted CI should provide more materials addressing availability and integrity concerns from the community, leveraging external expertise.
5. Trusted CI should document and share its experiences and expertise related to operating a community-focused center of excellence, to benefit other similar organizations.
6. When implementing our 2019-2023 vision, Trusted CI should emphasize outreach as an essential component of each strategic objective.

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

Round 1. 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)

Round 2. In 2Q2018, we received and accepted 4 applications for engagements. We accepted all four applications, with 3 planned for execution in the second half of 2018, and 1 scheduled for the first half of 2019.

- University of California-San Diego Scripps Institute of Oceanography (OCE-1327683; OCE-1212770; DEB-1556466; BCS-1745405; OCE-1756272)
- Environmental Data Initiative (DBI-1565103; DEB-1629233)
- Open OnDemand (OAC-1534949)
- SI2-SSI: SAGE2: Next Generation Integrated Persistent Visualization and Collaboration Services for Global Cyberinfrastructure (OAC-1441963)

Round 3. In 3Q2018, we opened and socialized the application (trustedci.org/application) for engagements to be executed in 1H2019. We received 6 applications, and accepted 4 applications for execution in the first half of 2019:

- Polar Geospatial Center (OPP 1559691; ACI 1614673)
- American Museum of Natural History (OAC 1827153)
- The Singularity Project, on behalf of the Open Science Grid (PHY-1148698; OAC-1836650; OAC-1827116; OAC-1841530)
- Purdue University (OAC - 1840043)

Additionally, in the 1H2019, we will be engaging the Scripps Institution of Oceanography (supports various NSF grants). We will be supporting the DOD-funded Principles-based Assessment for Cybersecurity Toolkit (PACT)[48] project who will be leading the assessment.

For a summary of all our planned, current, and past engagements, see Section 6: Table 5 and Table 6.

Table 3. Engagement Applications Received and Accepted

Round	**Execution Period**	**Applications Received**	**Applications Accepted**
1	1st Half of 2018	10	6[49]
2	2nd Half of 2018	4	4
3	1st Half of 2019	6	4[50]
	Totals:	***20***	***14***

[48] https://cacr.iu.edu/pact/
[49] 4 applicants agreed to a combined engagement
[50] Scripps is not counted in these four.

Plans for next year: In early 1Q2019, we will finalize detailed planning and begin execution of our 5[51] new engagements. We also will open and publicize a call for applications for engagements to be executed in the second half of 2019.

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" often 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. Consultations in 2018 were:

- A consultation with LSST on cybersecurity program frameworks and control selection.
- A consultation with Chester Langin from Southern Illinois University that resulted in a blog post[52].
- A consultation with Martin Greenwald of MIT regarding cybersecurity for a new project at MIT[53].

We neglected to report in prior reporting that in July of 2017 Trusted CI was invited to join the XSEDE Campus Champions email list. We have provided opinions on cybersecurity twice on that email list since joining.

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

3.3 Open Science Grid / HTCondor-CE

We applied our First Principles Vulnerability Assessment[54] (FPVA) engagement with The Open Science Grid (OSG, NSF PHY award #1148698)[55] to assess the security of HTCondor-CE (Compute Element) (NSF ACI award #1321762). We completed the Architectural (Component), and Resource diagrams, including privilege (`user`, `root`, other) information and then moved to step 4 of the methodology -- the detailed code inspection and analysis for vulnerabilities.

The assessment was carried out on the University of Wisconsin-Madison testbed, resulting in the discover of two vulnerabilities. The first one showed that a user process running on an executing machine could attack another user processes if both execute at the same time on the same machine. The second vulnerability allowed the user to perform a command injection

[51] This number includes a fifth engagement (Scripps) that was accepted in round 2 and deferred to 2019.
[52] http://blog.trustedci.org/2018/04/single-vs-multiple-users-on-cluster-node.html
[53] https://news.mit.edu/2018/mit-newly-formed-company-launch-novel-approach-fusion-power-0309
[54] https://research.cs.wisc.edu/mist/papers/VA.pdf
[55] https://www.opensciencegrid.org/

attack when submitting a job. To do so, the user could include malicious code in the arguments command of the submit description file.

We delivered a vulnerability report for each of the vulnerabilities found. In addition we delivered a report explaining all the explored paths, which constitutes parts of HTCondor-CE that are now considered to be less likely to be exploited.

The developers have since corrected the vulnerabilities that we identified and reported. The vulnerability that affected OSG was disclosed[56] .

3.4 National Radio Astronomy Observatory (NRAO)

In 1H2018, Trusted CI engaged with the National Radio Astronomy Observatory (NRAO)[57] (NSF Award # 1647378) to assess and facilitate the maturation of NRAO's information security program, positively impact the adaptiveness and longevity of their cybersecurity infrastructure and the trustworthiness of the science NRAO supports.

On an accelerated schedule to dovetail with NRAO's budgetary cycle, we completed an intensive fact-finding phase, performed a three-day on-site visit in Charlottesville, VA, and on April 16th delivered a preliminary report providing specific, prioritized actions that NRAO could take to bolster their security program.

Drawing from our preliminary report, David Halstead, CIO at NRAO, proposed a two-phase security budget plan to NRAO executives. Phase I included moving the current ISM into a CISO role and hiring a new security professional to report under him, as well as investing in additional network visibility tools, identifying key control systems that need further protections, and implementing a policy of "least privilege" for systems administrators and users. Phase II addresses long-term priorities and sustainability of the security program. David shared that Phase I had been tentatively approved by his management.

The final report that Trusted CI delivered included a set of foundational recommendations if they appeared feasible to begin in the next six months; called major resource additions or reallocations; and were expected to generate strong outcomes. We organized other recommendations by estimated benefit and cost to implement.

After delivering the final report, we used the remainder of our engagement time to facilitate phone and email discussions focused on implementing these recommendations and answer questions posed by NRAO about areas such as federated identity management, application

[56] https://opensciencegrid.org/security/vulns/OSG-SEC-2018-07-03-BLAHP-Vulnerability/
[57] https://blog.trustedci.org/2018/03/nrao-and-trusted-ci-launch-engagement.html

whitelisting, inventory and asset management, network visibility, and Trusted CI's process and tools for self-assessing gaps and actions using the CIS Controls v7.[58]

In the engagement evaluation, David Halstead cited a number of benefits to the engagement with the most impact being from the communication of risks to decision makers and stakeholders.

3.5 GenApp

GenApp[59] (NSF OAC award #1740097) is a tool for rapidly generating science gateways by providing a graphical frontend and associated server backend for command line scientific applications. GenApp-generated gateways run on dedicated local resources as well as cloud resources such as NSF Jetstream and Amazon Web Services. We began our engagement with the GenApp team January 2018 and completed the engagement June 2018.

The engagement focused on performing a security review of the GenApp codebase and the various web applications generated by GenApp, as well as evaluating the technologies and architectures utilized by the GenApp development framework. We worked with the GenApp team to create architectural diagrams, ran automated tools to analyze GenApp systems, and manually inspected key components of source code for vulnerabilities.

Findings included the need for more systematic sanitization of user input, keeping third-party libraries up to date, and recommendations for secure settings of web services of GenApp-generated applications.

The GenApp staff has graciously consented to publication of the engagement report after a sufficient period to implement suggestions for remediation of issues. We will contact GenApp towards the end of Q1 2019 to verify that issues have been addressed, after which the engagement report will be made available to the public. The hope is that other NSF-funded projects which are primarily software-based can learn from the tasks accomplished during this engagement.

3.6 Cloud Security Best Practices

Trusted CI, in collaboration with a community of academic cloud service providers, including: Agave Platform (TACC - NSF OCA-SS2-SSI-1450437), Cornell University Center for Advanced Computing (NSF CI-1541215), CyVerse (UA - NSF DBI-0735191, DBI-1265383), and Jetstream (IU - NSF 1445604), worked on identifying and documenting a set of security "best practices" for both operators and software developers responsible for academic clouds. The overarching goal was to improve cybersecurity for operators and users of academic clouds.

[58] https://blog.trustedci.org/2018/08/nrao-and-trusted-ci-complete.html
[59] https://genapp.rocks

A “cloud resource” within an academic institution provides a means for R&E users to run virtual machines or containers such that they can have a custom software stack and isolation from other users. Additionally, virtual machines or container images can be curated and provided by the cloud resource operator, they can be provided by the user, or they can be provided by a third party. This capability presents a number of challenges in the domain of cloud cybersecurity, e.g., users’ images are run with privileged access, images can be from unknown provenances, controls to reduce the risk an image may cause to both operator and other guests are limited, and managing security updates to images is cumbersome. To address these issues, the group produced the document, *Security Best Practices for Academic Service Providers*, published at http://hdl.handle.net/2022/22123.

In an effort to disseminate the newly identified best practices, we requested several operators to review our document and received feedback that we are currently processing. Similarly, Rion Dooley and John Michael Lowe presented our motivations, strategies and results reported in the document during the NSF Cybersecurity Summit in the form of a panel, moderated by Von Welch. Finally, Rion Dooley presented the document during Trusted CI’s December webinar.

Plans for next year: We will incorporate feedback we receive from reviewers of the document. LIkewise, we will pursue additional opportunities in disseminating the best practices document at other venues, e.g., OpenStack 2019.[60]

3.7 Environmental Data Initiative

The Environmental Data Initiative[61] (EDI) (NSF DBI award #1565103 and NSF DEB award #1629233) enables curation and archiving of environmental data, with emphasis on projects funded by NSF's Divisions of Biological Infrastructure and Environmental Biology. EDI provides support, training, and resources to help researchers archive and publish high-quality data and metadata. EDI operates a secure data repository and works closely with the Long Term Ecological Research Network (LTER) and DataONE to promote data management best practices.

The goals of this engagement were to review current authentication and authorization mechanisms, identify features and requirements for a future version of the EDI Data Portal and associated backend API, and document currently available authentication and authorization solutions.

We began Q3 2018 by negotiating the scope of the engagement to focus on the authentication and authorization scheme used by the PASTA+ API[62], and how it could be replaced by OAuth 2.0 / OpenID Connect (OIDC) authentication and alternative authorization mechanisms. We then

[60] https://www.openstack.org/summit/denver-2019/
[61] https://environmentaldatainitiative.org
[62] https://pastaplus-core.readthedocs.io

reviewed the current PASTA+ documentation and created basic architecture diagrams showing interaction between the EDI Portal and server backend. We identified portions of the current authn/authz system that need to be adapted to work with alternative login mechanisms based on OAuth protocols.

We then presented several OAuth-based identity providers and potential solutions to the current authorization scheme. These solutions included Google OAuth 2.0 with Google Groups, Globus Auth, ORCID OIDC, and CILogon 2.0. This activity was primarily one of knowledge transfer, and these potential solutions were gathered together in the engagement report delivered to EDI December 2018. EDI staff have kindly granted permission to make the report publicly available[63]. Selection of a new authn/authz framework and implementation of the updated EDI Portal was outside the scope of this engagement and will be performed by EDI staff sometime in the first half of 2019.

3.8 Open OnDemand

We are applying our First Principles Vulnerability Assessment[64] (FPVA) methodology to perform an in-depth vulnerability assessment of Open OnDemand (NSF award #1534949). This engagement started in Q3. So far 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. For this assessment initially we used a testbed at the University of Wisconsin-Madison, but as it was determined that that testbed was not representative enough of a real production testbed we continued the assessment at a testbed located at the Ohio Supercomputing Center (OSC). Open OnDemand allows friendly access to supercomputing resources. As it allows users to plug-in custom applications, we are looking for possibles attacks abusing that flexibility. This work is being carried out by Joe Atkins, a graduate student from UW-Madison.

Plans for next year: In the upcoming weeks, we will continue to run different tests with the objective of exploiting critical resources. We expect to finish this engagement in 1Q2019.

3.9 SAGE2

The Scalable Amplified Group Environment 2 (SAGE2) (NSF ACI Award 1441963) is a multi-site collaboration and visualization tool designed for use with tiled display walls. The mission of SAGE2 is to provide an innovative, user-centered, web-based platform for enabling local and/or distributed teams to display, manage, share, and investigate large-scale datasets on tiled display walls to glean insights and discoveries with greater speed, accuracy, comprehensiveness, and confidence.

[63] https://hdl.handle.net/2142/101921
[64] https://research.cs.wisc.edu/mist/papers/VA.pdf

The SAGE2 team applied to engage with us in April of 2018. They had identified a number of security objectives for their software they needed assistance in achieving. During initial fact finding it was determined that identity and access management issues would be the most impactful given the needs of their user community, the current state of the project, and the expertise of those involved in the engagement.

We considered a set of authentication and authorization approaches and made the decision to pursue OAuth 2.0 / OpenID Connect for SAGE2 with CILogon. As the majority of their users come from parent institutions in higher ed and research, CILogon provides broad coverage. The implementation of OAuth 2.0 and OpenID Connect also allows SAGE2 to integrate with a variety of other identity providers in the future if needed.

We carried out initial testing of software on Jetstream (NSF OAC Award 1445604) and Pittsburgh Supercomputing Center for CILogon integration testing. Once a working test was in place the SAGE2 team developed a demonstration to be used in presentations at SC 2018. Expertise developed in these exercises is being used to guide development efforts to integrate OpenID Connect with SAGE2. Work is ongoing and a working deployable docker container including SAGE2 with essential OpenID Connect functionality enabled is expected to be available in 1Q2019.

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 23 responses to our Engagement Evaluation Questionnaire[65] to date, including 11 responses in 2017 and 6 in 2018. This section begins with a summary of those responses in the aggregate, and then provides some analysis of select individual responses.

Section 4.1 provides an overall summary analysis of the responses. Sections 4.2 and 4.3 are analysis of specific recent responses from DKIST and the University of New Hampshire Research Computing Center respectively.

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 21 of 23 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 Trusted CI?”. The other 2 of rated 4 out of 5 (“Very Likely”) on Question 7.

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

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 23 responses include 19 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 23 responses in the aggregated summaries below for ease of analysis and to represent the full data set.

We consistently see high ratings of the positive impact of the engagement on the project or facility, and 21 of 23 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 Trusted CI?"

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

15 of 23 responses were 5. All 23 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 3 responses indicated any negative impact, with a rating of 1 ("low").

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:

- Increased cybersecurity knowledge among staff and personnel (16)
- Knowledge / documentation of information assets (15)
- Improved governance / policy / risk acceptance structure (14)
- Communication of risks to decision-makers and stakeholders (13)
- Understanding cybersecurity risks to the science mission (13)
- Selection of better technology or services (10)
- Improved security of software we are developing (8)
- More secure or efficient identity and access management practices (7)

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

- 7 responses indicated "Improved governance / policy / risk acceptance structure."

- 4 responses selected “More security or efficient identity and access management.”
- 3 responses selected “Communication of risks to decision-makers and stakeholders”
- 3 responses selected “Knowledge / documentation of information assets”

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.

10 responses selected “None.”
9 responses selected “Other priorities diverted attention from cybersecurity.”
6 responses selected “Insufficient project or facility resources applied to engagement.”
6 responses selected “Insufficient staff/budget/resources to make recommended changes.”

Q6. Which one of the barriers was most significant?

- 4 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 Trusted CI? (0 = Not Likely; 5 = Extremely likely)

21 of 23 respondents selected 5 (“Extremely likely”). 2 selected 4 (“Likely”)

Q8. Did the engagement with Trusted CI 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 5 ratings of 5. 22 of 23 responses were 3, 4, or 5. One respondent answered 0.

Q9. How does the Trusted CI 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**. 12 ratings of “much better”; 6 of “somewhat better”; 4 of “about the same”.
- **Quality of communication**. 13 ratings of “much better”; 5 of “somewhat better”; 4 of “about the same”.
- **Quality of deliverables**. 12 ratings of “much better”; 8 of “somewhat better”; 2 of “about the same”.
- **Positive impact on security**. 12 ratings of “much better”; 5 of “somewhat better”; 4 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.

15 of 23 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?

10 of the 23 responses had useful and constructive feedback on the Trusted CI engagement process to help us improve our process. The feedback ranged from knowledge we should obtain about dealing with large facility construction projects to tactics we can use to help better engage with the client. Many of responses to this question were complementary of our process.

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 2019.

4.2 DKIST Data Center Evaluation Analysis

The following summary was provided to Trusted CI by the DKIST Data Center:

> *The initial consultation with the engagement team can provide more pedagogical content for organizations whose executive management do not value cybersecurity best practices. This may help engagees better find resources to implement CS plans.*

Although the feedback from DKIST Data Center on our engagement was mostly positive, they did have a few helpful critical comments on how Trusted CI can improve on future engagements:

> *CTSC could more strongly evangelize the importance of cyber security best practices.*

One of the broader impacts of our engagement with DKIST Data Center was to have the opportunity to see their concise network map. DKIST allowed us to share the network map with the NRAO team as an example of how to make a network map.

4.3 UNH RCC Evaluation Analysis

The following summary was provided to Trusted CI by the University of New Hampshire Research Computing Center (UNH RCC):

> *Over this past year, RCC has worked to improve IT/Cyber security across numerous projects that comprise the UNH Research enterprise. As part of this effort,* ***RCC chose to make our response to the CTSC security recommendations our Wildly Important Goal for FY18.*** *[emphasis added] This focus on security allowed our staff to allocate enough time to make progress on many fronts.*
>
> *Highlights for RCC over the past year fall into two main categories: synergistic relationships and process improvements. Relationships progressed mostly through alignment with other UNH groups focusing on IT/Cyber security. Process improvements came from evaluating existing practices against current best practices and adopting those that were relevant to our domain.*
>
> *Moving forward, RCC intends to strengthen relationships with those accompanying us on this security journey by direct and appropriate management of client relations, utilization of subject matter experts from within and external to UNH, and through participation in IT/Cyber security education outreach initiatives for the UNH community.*
>
> *Many of our processes have improved, but a transformation momentum continues to drive us towards greater efficiency in addressing security. As the improvement life-cycle runs its course, we expect to accumulate security wins while at the same time freeing staff effort through automation.*

In the questionnaire responses, UNH RCC indicated that other priorities had been a factor in limiting the positive impact, and that the Trusted CI engagement was much better than any other cybersecurity assistance they had received.

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 a combination of funds directly from NSF, indirectly from NSF projects through subawards, e.g. by SGCI as described in Section

1.4, 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 is a significant step in this direction in that it demonstrates our perceived value by the community. In the latter part of 2018, Trusted CI and the CI Center of Excellence (CoE) Pilot[66] (NSF award #1842042, PI Deelman) co-funded a half FTE focused on cybersecurity, following the model Trusted CI has with SGCI. Through this collaboration Trusted CI provides advice to the CI CoE pilot by sharing our project management and engagement experiences, as well as cybersecurity expertise regarding identity management during the CI CoE's first engagement with NEON.

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[67] as well).

Funding received by Trusted CI participants that supports this funding diversity vision and is coherent with Trusted CI's mission includes:

- CI Center of Excellence (CoE) Pilot (NSF award #1842042, PI Deelman): shared .5 FTE.
- Science Gateways Community Institute (SGCI, NSF award #1547611, PI Wilkens-Diehr): shared .5 FTE.
- Infrastructure for Privacy-assured CompuTations (ImPACT)[68] (NSF award #1659367, PI Baldin): .1 FTE
- CICI: SSC: Securing Science Gateway Cyberinfrastructure with Custos (NSF award #1840003, PI Pierce): .1 FTE
- PFI-TT: Using Science Gateways to Enable Greater Access to High Performance Computing in Support of Advanced Manufacturing (NSF award #1827641, PI Pierce): .1 FTE
- DOD-funded Principles-based Assessment for Cybersecurity Toolkit (PACT)[69]: $2m/2 years is allowing for formalization and broadening the impact of engagement techniques.
- Professor Miller and Elisa Heymann receive approximately 0.1 FTE from UW-Madison to teach the software security course based on the materials developed under TrustedCI (see Section 2.5).

[66] http://cicoe-pilot.org
[67] See http://research.cs.wisc.edu/mist/includes/vuln.html
[68] https://renci.org/impact/
[69] https://cacr.iu.edu/pact/

5.2 REU Supplement from NSF

In 2017, Trusted CI received a Research Experience for Undergraduate (REU) supplement to fund students at IU and University of Wisconsin. The REU funding arrived too late to fund 2017 Summer students as planned and in consultation with NSF was repurposed.

At IU, we funded student Preston Ruff over the Summer of 2018 to mine the National Vulnerability Database for information on how common various CWEs (security vulnerabilities as identified in the Common Weaknesses Enumeration) are and identify what learning materials may aid programmers in our community best learn to avoid these most common errors. His results will be folded into the Software Engineering Guide (Section 2.7). It has already been used in software security trainings at the 2018 NSF Cybersecurity Summit and PEARC18.

At UW-Madison, the student assisted with current in-depth software assessment, Open OnDemand under the direction of Elisa Heymann (see Section 3.8).

5.4 Advisory Committee Changes and Meeting

The Trusted CI Advisory Committee 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 Trusted CI Advisory Committee was convened on November 12th, proximate to the SC18 conference. Kevin Thompson and Micah Beck attended and observed as representatives from NSF. The following guidance was given to Trusted CI by the Advisory Committee:

- Continue pursuing Service Center approach. Common need across Trusted CI, SGCI, etc.

- Ask for formal acknowledgement by engagees, e.g, during exit interviews.
- Give clear guidance about goals and evaluation process to fellowship applicants. Help them discern if they are an appropriate candidate to apply. Keep applicants engaged (e.g., a consolation prize for those not selected so they apply again next year).
- Expand transition to practice (TTP) engagements beyond Chicago. Include graduate students in these workshops, learning from the TTP workshop in NY.
- Position the Trusted CI Framework as complementary to NIST, rather than an alternative. Explore participation in revisions to 800-160 (resilience).
- Trusted CI coordination with ResearchSOC is a good thing. Current COI practices are good -- don't overdo it.
- Pay attention to branding/marketing around Trusted CI activities and related activities. Help steer people to the appropriate group for the services they need.
- Good to have a 5 year strategy but also remain agile/responsive to community needs. Have a process that enables the center to pivot in new directions.
- Report back to the Advisory Committee next year on adoption of Trusted CI assessment methodology outside of NSF (e.g., DoD/PACT).

We recently learned that Dr. David Halstead, CIO for the National Radio Astronomy Observatory will be resigning from the Advisory committee in 2019. Dr. Halstead has been a very valuable and active member of the committee and we thank him for his contributions to Trusted CI. A search will be conducted to find a replacement for this vacancy. Preferably someone with a strong ties to the Large Facility community.

5.5 Trusted CI All Hands Meeting

In mid June, we held our annual face-to-face All Hands Meeting in Chicago. We used the time together to review our successes, explore areas in need of improvement and future initiatives for 2019 and beyond. Major themes included a review of our five year vision and strategic plan, a presentation on the broadening impact and planning for the 2019 supplemental proposal. Several break out groups focused on Transition to Practice, NSF project relationships and software engineering in NSF CI.

5.6 Trusted CI Rebranding to Emphasize CCoE

In early 1Q2018 we rolled 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 was to emphasize the "NSF Cybersecurity Center of Excellence" title while maintaining any brand recognition in "Trusted CI" and avoiding confusion.

Launching the new name and logo involved updating the website, social media, and YouTube channel, releasing a blog post, and submitting press releases to relevant science and supercomputing publications.

Fig 8. New Trusted CI logo.

5.7 Assurance of Access Controls Within a Cloud Environment

A challenge that Trusted CI has faced that is not unique to any organization utilizing cloud services is in managing access to it's cloud storage document assets. We have applied the access control technologies available in Google Drive to limit access to data. For example, Trusted CI has a security policy requiring staff to use two factor authentication on parts of its document tree that contain sensitive documents such as those from Engagements. We also remove access for former members of our team when they depart the project.

However, Google Drive's UI is a bit quirky and has not always completely removed access for former colleagues when we have removed their access from top level folders. Some specific files would retain their old permissions. Also it is easy to inadvertently make files more broadly accessible, even public.

This was first discovered in Trusted CI by Mark Krenz when he used software he wrote to audit the permissions of Google Drive on Trusted CI's main folder as part of Trusted CI's ongoing cybersecurity program. This software, called "cloudperm"[70], uses Google Drive's API to list file metadata such as permissions in order to help in auditing access.

Mark further expanded upon this program in Q3 to include a method of revoking access in an automated fashion to the documents that the Google UI was not revoking access to through their UI. This allowed Mark to fix the access privileges on over 1700 documents in the Trusted CI document tree that otherwise would have remained undetected as a problem and exposed to former employee accounts had the software not been used.

[70] https://github.com/deltaray/cloudperm

Mark has also used the cloudperm software with SGCI in order to also check the permissions of documents within Google Drive to check for accidental exposure. SGCI has agreed to allocate a portion of Mark's Trusted CI time with SGCI to extend the reporting functionality of the software. In addition from benefiting from this software, we plan in the future to make the software known to other science projects who use Google Drive.

5.8 Personnel changes

- At IU, four new members joined the Trusted CI team: Ryan Kiser (Analyst), Anurag Shankar (Analyst), Zalak Shah (Analyst), and Diana Borecky (Event Coordinator).
- Craig Jackson has reduced his effort and withdrew as a co-PI to focus on cybersecurity assessments for the Department of Defence based on Trusted CI's work. Mark Krenz will be assuming some of Craig's leadership role.
- With mutual agreement, Scott Koranda from Spherical Cow Consulting left the project team. Since joining the project at its inception, Spherical Cow has achieved sustainable success and can provide the NSF community with identity management consulting directly. Trusted CI will continuing providing identity management expertise under the leadership of Jim Basney as needed.
- At UW-Madison, the student Sanjay Rajmohan was replaced with a more experienced student, Joel Atkins.
- Florence Hudson was hired as a consultant to work on Transitioning Cybersecurity Research to Practice as described in Section 1.8.

5.9 Supplemental Funding for 2019

A funded supplemental proposal (1842073) continues Trusted CI's activities through 2019 and expands its scope to add a Fellows Program (led by Dana Brunson at Oklahoma State), an effort to Transition Cybersecurity Research to Practice (led by Florence Hudson), and undertake an update expansion to the OSCRP as part of the Trusted CI Framework (led by Sean Peisert of Lawrence Berkeley National Laboratory (LBNL)).

While Oklahoma State and LBNL do not join Trusted CI until 2019, we have starting setting up subcontracts, onboarding, and adjusting meeting schedules to accommodate team members from LBNL (Pacific time zone). Florence Hudson joined Trusted CI in 3Q2018 to begin work on the Transition Cybersecurity Research to Practice by analyzing cybersecurity gaps in the NSF community which research could fill (see Section 1.8).

5.10 ResearchSOC Collaboration

Trusted CI PI Welch's proposal to establish the ResearchSOC, a collaborative security response center under CICI 18-547[71], was funded (NSF award #1840034) and he, along with co-PI Marsteller, have begun coordination between these two NSF cybersecurity centers. A set of operating coordination principles and collaborations was drafted by the Trusted CI and may be found in Appendix A.

5.11 Conflict of Interest Management

Trusted CI's success may be in part attributed to its ability to act as a trusted advisor to the community through its engagements, best practices, presentations, etc. With Trusted CI team members being members, and even leaders, on other cybersecurity projects, Trusted CI manages perceived conflicts of interest to help ensure its advice is trusted to be unbiased and not reflecting these memberships in other projects.

Specific practices include:

1. At the start of each Trusted CI management meeting, a standing agenda item is for everyone to disclose any new conflicts of interest.
2. When an engagement report makes a recommendation to a community member that includes a project that an author of the report is involved in, another unconflicted team member reviews the report for bias. A declaration is also included in the report, for example: "Conflict of Interest Declaration: One or more Trusted CI team members have a stake in technologies recommended or mentioned in this report, namely [e.g.] SWAMP and CILogon. This report has been reviewed and approved by unconflicted team members."

[71] https://www.nsf.gov/pubs/2018/nsf18547/nsf18547.htm

6 Metrics

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

Table 4. Trusted CI 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. Six engagements completed in 2018 (NRAO, GenApp, Cloud Security Best Practices, Environmental Data Initiative, Open OnDemand, SAGE2)
	Post-engagement survey.	High ratings of engagement utility.	On track. See Section 4.1 for new results.
	Consultations (new)	None.	3 (see Section 3.2)
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[72]. Aim to increase linearly.	The NSF Community Cybersecurity Benchmarking Survey performed by Trusted CI identified in 2018 that 6 projects are using the Trusted CI guide.
Cyberinfrastructure Vulnerabilities / *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 13 out of 25 Large Facilities represented on our list (52%). This is an increase of 2 over 2017.
	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.

[72] In 2019, we plan to modify this goal as we shift to the Trusted CI Framework described in Section 2.6

Table 4 (continued). Trusted CI activity goals and achieved metrics.

Activity	Measurement Technique	Goals	Achieved
Training	Direct measurement of attendance.	50 members of NSF community per year attending.	240 attendees from the NSF community attended training provided by Trusted CI staff. While this is a 178 attendee increase from the 2017 report, last year's metric only included 2017 NSF Summit attendees. 95 people attended the training sessions at the 2018 NSF Cybersecurity Summit. This is an increase of 33 from 2017. 81 people attended the Security Log Analysis and Incident Response training at Educause SPC. 18 people attended software assurance training at SC '18 28 attendees attended software assurance training at SecDev'18 12 attendees at Practical Cybersecurity Programs for Science Projects and Facilities at PEARC 18 6 attendees at Software Engineering training at PEARC '18
	Survey of attendees.	90%+ rating training as valuable.	Of the 38 people surveyed for the NSF Cybersecurity Summit training day, 94% of the attendees (36) said they would participate in training at future summits. 97% of the attendees (37) found the training useful. At Educause SPC: 7 of 7 attendees rated the Security Log Analysis training as good or excellent. 3 of 6 attendees surveyed rated the Incident Response training as good or excellent.

Table 4 (continued). Trusted CI activity goals and achieved metrics.

Activity	Measurement Technique	Goals	Achieved
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 55 NSF-funded projects including 21 large facilities. A decrease of 3 projects from last year but an increase of 3 large facilities over 2017. This is the largest number of large facilities recorded at a summit.
	CFP response rate.	Increasing CFP response rate each year.	The number of CFPs in 2018 was the same as last year's high of 32.
	Surveys of attendees.	Very strong evaluations on attendee surveys.	A post summit survey received responses from 51 attendees (6 more responses than 2017). To the question "How would you rate your overall experience with the 2018 summit?", 37 respondents answered that the quality of the summit was Excellent (highest rating), 12 answered Good (2nd highest) and 1 answered Average (3rd highest). This is a +9% point difference in the number of excellent responses from 2017.
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 2018, three applicants requested software assessments.
	Number of groups using online training materials	Linear progression each year.	Nothing to report yet.

Table 4 (continued). Trusted CI activity goals and achieved metrics.

Activity	Measurement Technique	Goals	Achieved
Outreach / Community Impact	Presentations at Project/PI Meetings	4-6 per year	On track, and exceeding. Presentations and sponsorship at PEARC '18 and SGCI Research Expo. NSF OAC and SCCI webinars. More presentations at SGCI bootcamp, SPACI@MSIs, Internet2 Global Summit, EDUCAUSE Security Professionals workshop,
	Mentions in NSF Solicitations	Goal is all solicitations with a requirement for a cybersecurity program to mention us as a resource.	Two: NSF 18-547 and 19-514. Plus pointer to Trusted CI on Large Facility Office website.
	Webinar attendance and views of archives (new)	Continued growth	Attendance: 299 Archive views: 908
	Subscribers to Trusted CI email Lists (new)	Continued growth	Announce: 699 (+82 since 2017) Discuss: 422 (+94 since 2017)
	Large facilities participating in Large Facilities Security Team (new)	Goal is to have all Large Facilities participating.	22/25 participating

7 List of All Trusted CI Engagements

Table 5. All Trusted CI 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.
DataOne	ACI #1430508	Cyber checkup
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.
Environmental Data Initiative	NSF DBI Award #1565103 and NSF DEB award #1629233	Reviewed current authentication and authorization mechanisms, identify features and requirements for a future version of the EDI Data Portal and associated backend API, and document currently available authentication and authorization solutions.
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.

Table 5 (continued). All CTSC Engagements (in progress and completed) under current award

Engaged Project	NSF Award # or Category	Engagement Subject
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.
Multi-Institutional Open Storage Research Infrastructure (MI_OSiRIS)	1541335	Federated identity and access management.
Open OnDemand	1534949 and 1835725	We are applying our First Principles Vulnerability Assessment (FPVA) methodology to perform an in-depth vulnerability assessment of Open OnDemand
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.
SAGE2	ACI Award 1441963	Identity Management consultation
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.

Table 5 (continued). All CTSC Engagements (in progress and completed) under current award

Engaged Project	NSF Award # or Category	Engagement Subject
Wildbook/IBEIS	1550881	Collaborated on the development of a role-based access control (RBAC) prototype for the next generation Wildbook platform.

Table 6. CTSC (Trusted CI) 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 6 (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.

Appendix A - Trusted CI - ResearchSOC Coordination

From the Trusted CI Policy document on coordination between the Trusted CI and ResearchSOC:

Observations

- **The centers' goals are aligned**: Both centers strive to enable the NSF community to successfully manage cybersecurity risks and produce trustworthy science. While the centers take different approaches toward these goals, their efforts are complementary.
- **The centers' identities are distinct**: ResearchSOC is primarily offering limited operational security services. Trusted CI is primarily focused on cybersecurity programs and NSF community cybersecurity support.
- **The centers have different needs regarding impartiality:** ResearchSOC, as part of its mission, seeks to foster adoption of its set of technology services. Trusted CI intentionally seeks to be a trusted, unbiased source of recommendations regarding cybersecurity.
- **Trusted CI already has processes for managing COI:** The Trusted CI PIs are involved in projects external to Trusted CI and have processes in place for managing any COIs created by those roles.

Collaborations

- Open Science Cybersecurity Framework (OSCF)
    - ResearchSOC's services address some of the topic areas in Trusted CI's Framework, but a ResearchSOC subscription by itself does not constitute a cybersecurity plan.
    - Trusted CI's Framework is expected to recommend ResearchSOC's services alongside alternative options.
- NSF Cybersecurity Summit
    - Organized by Trusted CI
    - ResearchSOC will attend, submit content
- ResearchSOC should adopt current Trusted CI best practices/training.
- Cyberinfrastructure Vulnerability Service.
- Outreach to higher education to improve the understanding of information security for research and research computing.

Principles

- **Trusted CI and ResearchSOC should collaborate as much as possible to make efficient and effective use of resources.** NSF 19-514 calls for as much: "A Cybersecurity Center of Excellence (CCoE) must: … Coordinate with the NSF-funded

Collaborative Security Response Center (CSRC, which provides operational services and intelligence to NSF projects), refine existing threat models identifying the vulnerabilities in NSF-funded cyberinfrastructure and scientific data associated with that cyberinfrastructure, and recommend countermeasures to protect the systems;"

- **ResearchSOC should clearly differentiate itself from Trusted CI when promoting its services.** When preparing promotional materials, use the appropriate logo(s). In presentations, speakers should clearly identify the organization(s) they are representing.
- **ResearchSOC should strive to be of sufficient quality and value to the NSF community such that Trusted CI co-PIs do not have concerns in including it as an option in Trusted CI materials.**
    - Trusted CI will provide honest, objective feedback to the ResearchSOC.
- **Current Trusted CI COI Management Processes should be strengthened as needed to accommodate these principles.**