



Annual Report for 2019 / Project Year Four

Trusted CI

The NSF Cybersecurity Center of Excellence

NSF Grant ACI-1547272

January 1, 2019 - December 31, 2019

For Public Distribution

Trusted CI Team

Ishan Abhinit<sup>2</sup>, Andrew Adams<sup>1</sup>, Kay Avila<sup>3</sup>, Jim Basney<sup>3</sup> (co-PI), Kathy Benninger<sup>1</sup>, Leslee Bohland<sup>2</sup>, Dana Brunson<sup>5</sup> (co-PI), Diana Cimmer<sup>2</sup>, Robert Cowles<sup>7</sup>, Jeannette Dopheide<sup>3</sup>, Terry Fleury<sup>3</sup>, Reinhard Gentz<sup>6</sup>, Grayson Harbour<sup>2</sup>, Dr. Elisa Heymann<sup>4</sup>, Florence Hudson<sup>7</sup>, Craig Jackson<sup>2</sup> (co-PI), Ryan Kiser<sup>2</sup>, Benjamin Kinzer<sup>4</sup>, Evan Kivolowitz<sup>4</sup>, Mark Krenz<sup>2</sup>, Prof. Barton Miller<sup>4</sup> (co-PI), Sean Peisert<sup>6</sup>, Scott Russell<sup>2</sup>, Raghav Sethi<sup>3</sup>, Zalak Shah<sup>2</sup>, Anurag Shankar<sup>2</sup>, Kelli Shute<sup>2</sup>, Susan Sons<sup>2</sup>, Von Welch<sup>2</sup> (PI), John Zage<sup>3</sup>

<sup>1</sup> Carnegie Mellon University/PSC

<sup>2</sup> Indiana University/CACR

<sup>3</sup> University of Illinois/NCSA

<sup>4</sup> University of Wisconsin-Madison

<sup>5</sup> Internet2

<sup>6</sup> Lawrence Berkeley National Lab

<sup>7</sup> 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, transition-to-practice guidance, training and best practices disseminated to the community through webinars, a fellows program, 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>

To reference the Trusted CI project, please reference the following paper:

Andrew Adams, Kay Avila, Jim Basney, Dana Brunson, Robert Cowles, Jeannette Dopheide, Terry Fleury, Elisa Heymann, Florence Hudson, Craig Jackson, Ryan Kiser, Mark Krenz, Jim Marsteller, Barton P. Miller, Sean Piesert, Scott Russell, Susan Sons, Von Welch and John Zage. Trusted CI Experiences in Cybersecurity and Service to Open Science. PEARC'19: Practice and Experience in Advanced Research Computing, 2019. <https://doi.org/10.1145/3332186.3340601>

## About This Report

This report represents project year 4 (PY4) of Trusted CI under NSF grant 1547272, which was aligned with calendar year 2019. This is the final year of grant 1547272 and the last expected annual report for this grant. The Trusted CI project will continue in 2020 under funding from a new NSF grant award 1920430. This report does not contain any significant future plans for that award, those plans being documented in our proposal to NSF which resulted in the new award, and in a performance execution plan being delivered to NSF in late 2019. Prior to grant 1547272, Trusted CI was supported under NSF grant 1234408.

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.

This work is made available under the terms of the Creative Commons Attribution 3.0 Unported License. Please visit the following URL for details:

[http://creativecommons.org/licenses/by/3.0/deed.en\\_US](http://creativecommons.org/licenses/by/3.0/deed.en_US)

Please cite this report as:

Trusted CI Annual Report for 2019. December 2019. <http://hdl.handle.net/2022/24873>

For updates to this report and other reports from Trusted CI, please visit

<https://trustedci.org/reports/>

## Trusted CI 2019 Highlights

- A. The 2019 NSF Cybersecurity Summit was executed by Trusted CI from October 15th through the 17th in San Diego, CA. A new high was seen for the plenary with 143 people in attendance. Ninety-one people attended the opening training and workshop day.
- B. The new Trusted CI Fellows program was launched, announcing its inaugural cohort in mid-April and holding a 20-week Virtual Institute for those Fellows.
- C. Jim Basney of NCSA, a founding Trusted CI team member, assumed the role of Trusted CI Deputy Director. The Trusted CI team also welcomed Internet2, represented by Dana Brunson, and LBNL, represented by Sean Peisert.
- D. The 2019 cybersecurity transition to practice workshop was held June 19th in Chicago, hosted by Microsoft and co-sponsored by Trusted CI, Box and the Indiana University Research and Technology Corporation.
- E. The Large Facilities Security Team (LFST) has designated representatives from each of NSF's twenty "Major Facilities" programs and/or their twelve associated subprograms.
- F. Ewa Deelman, Michela Taufer, Victoria Stodden, and Von Welch published a paper entitled Initial Thoughts on Cybersecurity and Reproducibility and presented at the 2nd International Workshop on Practical Reproducible Evaluation of Computer Systems (P-RECS19).
- G. Trusted CI is now partners with the EDUCAUSE Higher Education Information Security Council (HEISC). This partnership will result in additional dissemination of Trusted CI activities and products to the HEISC community.
- H. Trusted CI's work was prominently and positively mentioned by the NSF's OAC CI COE Program (PD 20-139Y) and continues to be listed on the NSF Large Facilities Office website.
- I. The Trusted CI webinar series hosted eleven talks with 357 total attendees and over 1200 views of previous webinar recordings.
- J. We held two calls for engagement applications, receiving 18 total applications and accepting 9. We completed engagements with REED+ (Purdue University), the Singularity Project, Polar Geospatial Center, American Museum of Natural History, Scripps Institute of Oceanography, Globus, SLATE, United States Academic Research Fleet, and UNAVCO. We have four engagements scheduled for the first part of 2020: Franklin & Marshall, UCB Secure Research Data and Computing, Open Storage Network, and XSEDE Metric Service.

- K. 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 27 of 31 responding 5 out of 5 (“Extremely likely”) and the other four responding 4 out of 5 (“Very Likely”).
- L. Our Cyberinfrastructure Vulnerabilities program issued 25 cyberinfrastructure vulnerability alerts to 144 subscribers, as well as added our first non-funded security analyst to our discussion list.
- M. Presentations and trainings were delivered at EDUCAUSE Security Professional Conference, Internet2 Global Summit, the SGCI Bootcamp, the University of Iowa, the NSF Cybersecurity Summit, PEARC19, the Gateways’19 conference, SFSCon, SuperComputing’19, Internet2 TechEx, the Science Gateways Community Institute webinar, the 2019 NSF Large Facilities CI Workshop, the U.S. European Command JCC International Cyber Summit, and the 2019 Great Plains Networks All-Hands Meeting.

# Table of Contents

<b>About Trusted CI</b>	<b>1</b>
<b>About This Report</b>	<b>2</b>
<b>Trusted CI 2019 Highlights</b>	<b>2</b>
<b>Table of Contents</b>	<b>5</b>
<b>1 Building Community</b>	<b>7</b>
1.1 NSF Cybersecurity Summit	7
1.2 Large Facility (LF) Outreach	10
1.3 Webinar Series	12
1.4 Science Gateways Community Institute Partnership	13
1.5 Trusted CI at PEARC	15
1.6 CI CoE Pilot Collaboration	15
1.7 Benchmarking Survey	16
1.8 Presentations	17
1.9 Cybersecurity Research Transition to Practice	20
1.10 Social Media Impact	23
<b>2 Sharing Knowledge</b>	<b>24</b>
2.1 Open Science Cyber Risk Profile	24
2.2 Situational Awareness / Cyberinfrastructure Vulnerabilities	25
2.3 Publications	26
2.4 Training	27
2.5 Software Security Course Development	30
2.6 The Trusted CI Framework: An Architecture for Cybersecurity Program	32
2.7 Secure Software Engineering Guide	33
2.8 Broader Impacts	33
2.9 Fellows Program	34
2.10 Law and Policy Insights	36
<b>3 One-on-One Collaborations: Engagements</b>	<b>37</b>
3.1 Engagement Applications	37
3.2 Consultations	38
3.3 REED+	38
3.4 American Museum of Natural History	39
3.5 Polar Geospatial Center	40

3.6 Scripps Institution of Oceanography	41
3.7 Singularity	42
3.8 Globus	42
3.9 SLATE	43
3.10 U.S. Academic Research Fleet	44
3.11 UNAVCO	44
<b>4 Engagement Evaluations</b>	<b>45</b>
4.1 Quantitative Results	45
4.2 Qualitative Results	47
<b>5 Lessons Learned, Challenges, and Project Management</b>	<b>49</b>
5.1 Follow-on Funding Award under Award 1920430	49
5.2 Basney Named Trusted CI Deputy Director	49
5.3 New Subawards: Internet2 and LBNL	49
5.4 Advisory Committee Changes and Meeting	50
5.5 Trusted CI All Hands Meeting	52
5.6 Personnel changes	52
5.7 ResearchSOC Collaboration	53
5.8 Sustainability	53
5.9 Trusted CI Incident Response Report 2019-10-02_01	54
<b>6 International Travel and Impact</b>	<b>55</b>
<b>7 Metrics</b>	<b>55</b>
<b>8 List of All Trusted CI Engagements</b>	<b>59</b>

# 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 2019 NSF Cybersecurity Summit<sup>1</sup> was executed by Trusted CI October 15-17 in San Diego, CA. The summit was built on the success, findings, and lessons learned from previous years. The summit had record attendance on the plenary days with 143 attending (a 25% increase from 117 in 2018); 91 attendees joined us on the training day.

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 attendees represented 57 NSF projects.

The Summit keynote speaker was Stefan Savage, who was invited by the program committee. In his presentation titled "Advancing Cybersecurity as an Evidence-based Discipline", he spoke about the disconnect between security researchers and operators and how cybersecurity attackers are easier to measure than defenses. The keynote was well received by the audience as 62% of those surveyed indicated it as one of their favorite parts of the conference.

Continuing on the strategy from 2018, a modest fee of \$200 was charged to attend the Summit to help cover costs that were not accounted for in the initial grant funding. Trusted CI also continued with the code of conduct from the previous year to help be proactive about potential issues and set the tone for expectations by attendees so that they feel welcome and safe at the Summit.

Feedback for the Summit and training sessions was very positive with 97% of surveyed attendees reporting the summit experience as "Excellent/Good" and 87% indicating that they would like to attend future Summits.

The first day consisted of training and workshops organized by Trusted CI and others responding to our call for participation:

- Web Security and Automated Assessment Tools - Theory and Practice, Barton P. Miller and Elisa Heymann
- Security Log Analysis, Mark Krenz and Ishan Abhinit

---

<sup>1</sup> <https://trustedci.org/summit>

- Setting Up a Compliance Program for CUI; Regulated Data Security and Privacy: DFARS/CUI, HIPAA, FISMA, and GDPR, Anurag Shankar, Gabriella Perez, Scott Russell and Erik Deumens
- Catch the Phish: Securing Your Organization Against Phishing Attacks, Rajvardhan Oak
- WISE Workshop, WISE Community
- Jupyter Security, Rick Wagner, Matthias Bussonnier, Mark Krenz and Ishan Abhinit
- ICS Security Landscape - Getting Better, Getting Worse, Phil Salkie
- A Cybersecurity Program Framework for Science Projects and Facilities, Craig Jackson, Bob Cowles, Kay Avila
- Social Engineering Workshop, Aunshul Rege, Rachel Bleiman and Trinh Nguyen
- Operational Fundamentals: Next Level Incident Response, Security Exercises, and Cybersecurity Operational Metrics for Science Projects, Susan Sons

New this year at the summit were two sessions during the plenary with different formatting. One event was an hour devoted to 7 lightning talks. The second was a plenary talk by Romain Wartel titled "15 Years of Attacks Against our Community: The Phalanx and Windigo saga", which was designated as Traffic Light Protocol (TLP)<sup>2</sup> "RED". Both of these new sessions received praise in surveys and we plan to look for ways to include these types of sessions in future summits.

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 half day workshop during the training day open to all Summit attendees combining informational and interactive activities including:

- Introduction to WISE
- The Security Communications Challenge Coordination Working Group
- Operational security and sharing threat intelligence
- Security for Collaborating Infrastructures - the WISE SCI working group.

The WISE workshop hosted at the summit enabled the collaboration and exchange of operational practices between US and European based Cyberinfrastructure communities.<sup>3</sup>

As in prior years, Trusted CI organized a student program at the Summit to follow through on our goals of outreach and broadening impact. Students apply to the program by writing a brief

---

<sup>2</sup> <https://www.us-cert.gov/tlp>

<sup>3</sup> <https://wiki.geant.org/display/WISE/WISE+@+NSF+Cybersecurity+Summit+2019>

essay sharing their security interests and what they hope to gain from the Summit. This year, the committee received twenty applications (up from seven applications last year). In addition to an increase in applications, there was an increase in applicant quality and diversity. While we traditionally accept 5 students in the program, we accepted 10 students to the program this year. Some excerpts of their feedback from the experience are below:

*“For me, I learned so much! I got actual experience with security tools in a real world setting in the Web Security Automated Assessment Tools session. I enjoyed speaking further with Dr. Miller about graduate school and I actually scheduled a visit to the University of Wisconsin-Madison. Furthermore, I appreciated being treated like a professional in the field although I am still a student. Being asked the difficult questions and being forced to put things into the perspective of a real world event on the spot was intriguing, challenging, and inspiring. It also showed me that I have much to learn in every aspect of this field! I am much more confident in my degree choices now because I attended this summit and got real feedback and honesty when it came to me asking the right questions, giving the right answers, and even thinking in the correct way in order to be successful in this field. Everything I wanted to get out of this summit was achieved!”*

*“Being able to attend this summit was a wonderful experience and I would recommend any student interested in Cyber Security to attend. The staff at IU and Trusted CI were very welcoming and gracious. Along with being wonderful to me, they were extremely organized and punctual throughout the summit. You will be able to network with many research individuals in the cybersecurity field. The training session was only 3.5 hours long each but the presenters did a great job of overloading us with great information and allowing us to do many hands-on exercises in the process. If you have the opportunity to attend this event. I greatly encourage it.”*

*“I have attended a couple of conferences before: this summit was a bit different for me. Apart from the usual knowledge hunting, I have got great networking opportunities here. I would specifically mention about my fellows in student programs and mentors. My mentor was superb: I felt really inspired after meeting her. About the conference contents, I liked the training program most: the hands-on training was useful and informative. I would remember this summit for good training and informative plenary sessions as well as a super awesome networking environment.”*



**Figure 1. Student attendees at the 2019 NSF Summit**

A more comprehensive report of summit activities and outcomes will be published in January 2020:

Andrew Adams, Kay Avila, Kathy Benninger, Jeannette Dopheide, Mark Krenz, James Marsteller, and John Zage. Report of the 2019 NSF Cybersecurity Summit for Cyberinfrastructure and Large Facilities: <http://hdl.handle.net/2142/105533>.

## 1.2 Large Facility (LF) Outreach

The Large Facility Security Team (LFST) continued to meet on a monthly basis, featuring a topic of interest relating to cybersecurity. In the first quarter of the year the LFST reviewed the draft NSF's Major Facility Guide (MFG) that was released for public comment in late December of 2018. Many members of the team were hoping for more prescriptive guidance relating to *Section 6.3 Guidelines for Cyber-Security* than what was in the draft MFG. After several discussions with the LFST, Trusted CI submitted comments to section 6.3 of the draft MFG. While the published draft provides less detail and specificity than our most recent drafts, we believe much of the content is well-aligned with Trusted CI's advice and experience working with the community. The response can be found in detail on the Trusted CI Blog<sup>4</sup>. LFST talks in the first quarter also included DNS hijacking and mitigation strategies, and a presentation by Ewa Deelman from USC on the NSF-funded pilot project to plan a Center of Excellence in Cyberinfrastructure.

Talks for the LFST in the second quarter included a presentation on different types of intrusion detection systems, tools, and approaches and a preview of the Trusted CI Framework. A milestone was hit in this quarter: for the first time since inception we now have representation

---

<sup>4</sup> <https://blog.trustedci.org/2019/02/comments-on-nfs-major-facilities-guide.html>

from all of the Major Facilities and/or their subprograms. With 100% representation, we'll look at how to best serve Mid-scale projects.

The MFG, as it neared approval, was revisited in the LFST third quarter talks. Risk acceptance was also discussed in this quarter with some of the LF sites shared their organizations' approaches to risk management policy. Rounding out LFST talks for 2019 during the fourth quarter were presentations about the Services Layer at the Edge (SLATE) platform and Identity Management (IdM). SLATE is currently in a requirements identification stage while IdM is focusing on fostering a community-driven approach to solving IdM challenges across the LFs and creating a central repository of knowledge.

Co-PI James Marsteller attended the 2019 Large Facilities Workshop (LFW) in Austin, Texas, in early April as the Trusted CI representative. He presented a lightning talk on the last day of the workshop and participated in a poster session highlighting the Trusted CI *Guide to Developing Cybersecurity Programs for NSF Science and Engineering* project that was developed with an engagement with the Daniel K. Inouye Solar Telescope (DKIST). Marsteller responded to a request from the Large Facilities Office seeking assistance with planning for the 2020 LFW.

In the fourth quarter Marsteller and Kathy Benninger responded to a request from the NSF Large Facility Office (LFO) to share experiences and lessons learned through outreach and facilitating Trusted CI's LFST team interactions.



**Figure 2. LFST Group Photo from NSF Cybersecurity Summit (16 October 2019)**

### 1.3 Webinar Series

The monthly CCoE Webinar Series<sup>5</sup> continued into 2019. Table 1 shows the number of webinar attendees and archive viewers in 2019.

**Table 1. Trusted CI Webinar attendance and archive viewing.**

<b>Date</b>	<b>Topic</b>	<b>Speaker(s)</b>	<b>Attended<sup>6</sup></b>	<b>Watched Later<sup>7</sup></b>
Jan.	The ResearchSOC	ResearchSOC Leadership Team	61	71
Feb.	Anticipatory Cyber Defense	Jay Yang	24	48
Mar.	NSF CC-DNI SecureCloud	Casimer DeCusatis	17	43
Apr.	REED+ Framework	Preston Smith	81	101
May	Deployable Internet Routing Security	Amir Herzberg	28	62
June	The Trusted CI Framework:	Craig Jackson, Bob Cowles	34	59
July	Ancile: Enhancing privacy	Jason Waterman	9	9
Aug.	SWIP	Mandal & Rynge	21	34
Sept.	Jupyter Security	Thomas Mendoza	49	60
Oct.	GDPR, 1 Year Later	Scott Russell	19	71
Dec. <sup>8</sup>	DDIDD Project	John Heidemann	14	No data yet
<b>Total</b>			<b>357</b>	<b>558</b>

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 2019, the videos from our series received approximately 2973 views, up from 908 views in 2018. This number includes views of presentations recorded prior to 2019.

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 2019, we added 130 subscribers to “announcements” and 126 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

<sup>5</sup> <https://trustedci.org/webinars/>

<sup>6</sup> Does not include Trusted CI staff and presenters.

<sup>7</sup> Viewed later on YouTube

<sup>8</sup> 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.

during the year. This targeted outreach strategy has the added benefit of Trusted CI helping promote the NSF CICI program. In 2019 we scheduled at 7 CICI awardee projects.

## 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. This collaboration includes consultations, training, and security services.

Consultations are achieved through SGCI's Incubator project. In 1Q2019, Trusted CI staff initiated engagements with four projects, including: EarthCube's Data Discovery Studio -- they sought a security review of their server and website<sup>9</sup>. We provided them with a written set of recommendations to improve their security; UCSD's School of Medicine, who required advice on their project, GAGE-DB, interaction with the Box file storage cloud service.<sup>10</sup> We reviewed their implementation of Box folder permissions and provided general high level cybersecurity advice for the project overall; The Rolling Deck to Repository collaboration, which seeks best practices in transferring and archiving data<sup>11</sup>; and the developers of SeedMe2 -- they requested advice in penetration testing and we provided advice and guidance on the use of software penetration testing tools<sup>12</sup>. COSMIC2, which requested a security review of their website, image processing tools, and servers. We are currently in the middle of this review.

Along with consultations through the Incubator project, we additionally provide security services to SGCI. Trusted CI has been tasked with performing periodic audits of SGCI's cloud document store in order to check their permissions and provided a report, highlighting those that had open permissions that could potentially be viewed by unauthorized individuals. To this end, SGCI further expressed interest in utilizing and developing the "cloudperm" software created by Trusted CI staff to perform the scan, and are contributing a portion of Trusted CI's effort to extend the reporting functionality of the cloudperm software.

Trusted CI also monitors the SGCI's websites for known vulnerabilities and weaknesses and provides input on cybersecurity matters when they arise within the group.

---

<sup>9</sup> <https://www.earthcube.org/group/earthcube-data-discovery-hub>

<sup>10</sup> <https://medschool.ucsd.edu/som/psychiatry/research/BRAIN/Pages/default.aspx>

<sup>11</sup> <https://www.rvdata.us/>

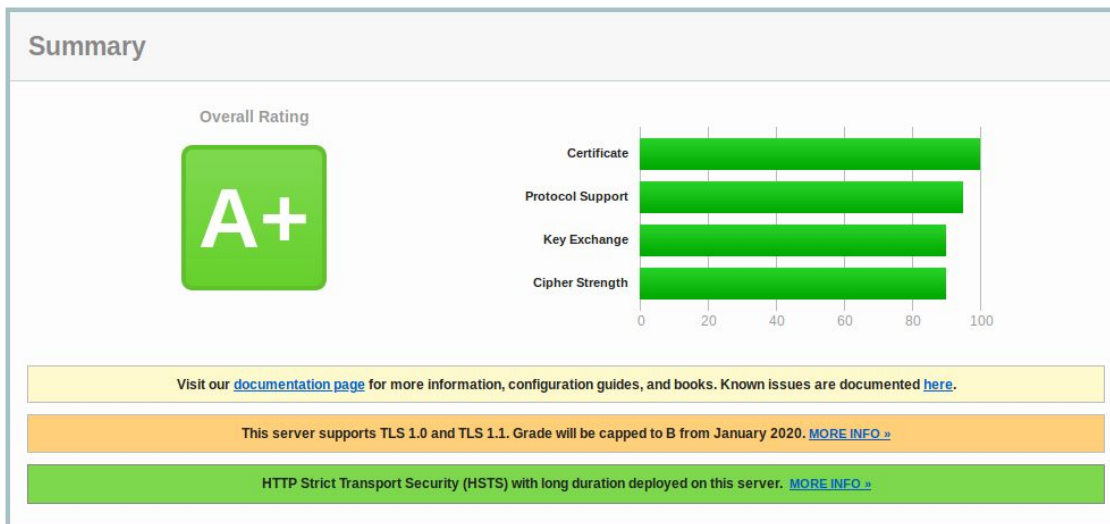
<sup>12</sup> <https://dibbs.seedme.org/>

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > sciencegateways.org

## SSL Report: sciencegateways.org (129.114.99.210)

Assessed on: Thu, 19 Dec 2019 15:08:08 UTC | HIDDEN | [Clear cache](#)

[Scan Another »](#)



**Figure 3. Screenshot from Qualys SSL Labs tool, showing that the website sciencegateways.org has received an A+ rating for it’s SSL security.**

Mark Krenz from Trusted CI also presented an hour-long training workshop on cybersecurity at two SGCI bootcamps. Bootcamp #5 took place in Indianapolis in May. It was attended by 18 operators representing 8 different science gateways. Mark used hands-on exercises designed to help guide participants through the process of identifying cybersecurity risks in their organization. Survey results from the camp showed that 14 of 16 who responded indicated they learned something about cybersecurity that will benefit their gateway. According to the survey, one of the audience members identified that one of their takeaway moments from the week-long bootcamp covering technical and non-technical topics was essentially that their prioritization of cybersecurity would also benefit their fundability and audience uptake, which was one of the points Mark made in his session. The social functions of the boot camp also allowed Mark to discover a gateway, Data Nomination Tool<sup>13</sup>, that helps to identify data repositories for research projects which are at risk of losing their data. This service can be used as a security mitigation to address long-term availability.

Bootcamp #6 took place in Chicago in September. It was attended by 9 operators representing 3 different science gateways. Mark reused much of the cybersecurity content from bootcamp

<sup>13</sup> <https://dataatrisk.org/>

#5. All attendees of the bootcamp rated the presentation as helpful to their understanding of cybersecurity for their gateway.

## 1.5 Trusted CI at PEARC

Trusted CI continued its active role at PEARC<sup>14</sup>, which was held in Chicago on July 28 - August 1. Trusted CI sponsored PEARC19 at the bronze level, which included an exhibit table. The convenient location in 2019 enabled us to send more Trusted CI staff than in previous years.

Below is a summary of Trusted CI's participation in the PEARC19 program:

- The paper, "Trusted CI Experiences in IT Security and Service to Open Science<sup>15</sup>," describes experiences, lessons learned, and future vision for the project.
- A panel, "NSF Centers of Expertise PEARC19," which brought together leaders of centers for expertise serving the CI and NSF communities to present, explore challenges, and ultimately foster greater engagement with the community. Participants included Trusted CI, the ResearchSOC, the Science Gateway Community Institute, the Molecular Sciences Software Institute, and the Engagement and Performance Operations Center.
- The workshop, "Trusted CI Workshop on Trustworthy Scientific Cyberinfrastructure," was an opportunity to share experiences, recommendations, and available resources for addressing cybersecurity challenges in research computing.
- The poster, "Trusted CI, the NSF Cybersecurity Center of Excellence," is a summary of Trusted CI's mission, to provide 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 effective cybersecurity programs.
- Florence Hudson participated in a panel during the AI4GOOD workshop, which examined privacy, policies, security, and ethics regarding artificial intelligence.

## 1.6 CI CoE Pilot Collaboration

With the funding of the CI Center of Excellence (CoE) Pilot (NSF award #1842042, PI Deelman) in the latter half of 2018, the Pilot and Trusted CI began a collaboration based on the 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. Outcomes from the collaboration during this quarter include:

- The Centralized authN/Z solution for the NEON data portal – leveraging OpenID Connect, CILogon, and Auth0 – which were completed last quarter have now been deployed to production.

---

<sup>14</sup> <https://www.pearc19.pearc.org/>

<sup>15</sup> <https://doi.org/10.1145/3332186.3340601>

- The CI CoE Pilot IdM team announced their upcoming IdM working group at a meeting of the Trusted CI Large Facilities Security Team on December 12, 2019. Beginning in January 2020, the IdM Working Group will meet to facilitate discussions between persons working with Identity Management in and across NSF Large Facilities to address IdM challenges that broadly impact the Large Facilities ecosystem.
- A weekly co-learning workshop is being held between members of the working group where topics and technologies in IdM can be researched and discussed in depth for inclusion in a planned IdM knowledge base website.

## 1.7 Benchmarking Survey

In 2016, we began socializing and collecting responses on a benchmarking survey designed to collect and aggregate information about cybersecurity in the NSF science community. The goal was to provide the 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.<sup>16</sup>

In September 2018, the team decided to shift the Survey to a 2 year cycle, circulating the Survey in the Spring and producing the Report in the Fall, and focusing the Survey on Major Facilities (formerly “Large Facilities”) and other large science projects.

In Winter 2019 we began coordinating the Community Survey with the Trusted CI Framework project (see Section 2.6), and incorporated the provisional “Musts” from the Trusted CI Framework into the Survey Questionnaire.

The survey was announced on May 23, 2019 on the Trusted CI “Announce” mailing list. The survey was further promoted on Trusted CI’s Blog on July 3, 2019, through the XSEDE mailing list, and during the Large Facility Security Team meetings during the months of May, June, and July. Reminders were posted to the Trusted CI Announce email list on July 18, July 29, and July 31. The response period to the survey closed on July 31, 2019.

Preliminary findings for the 2019 Survey Report were circulated in Oct 2019 within Trusted CI, and the final Survey Report is scheduled to be published in the first week of January 2020.<sup>17</sup>

The 2019 Survey continued 2017’s trend of a high response rate from NSF Major Facilities, with 14 of the 23 respondents being MFs. (The 2017 Survey had 15 of 20 respondents as Large Facilities; 2016 had 9 of 27.) Other noteworthy findings include: multi-factor authentication

---

<sup>16</sup> 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>.

<sup>17</sup> “2019 NSF Community Cybersecurity Benchmarking Survey Report,” <http://hdl.handle.net/2022/24912>.

continued its upward progress in adoption rates, with ~75% of respondents utilizing the control (contrast with 60% in 2017 and 22% in 2016); average cybersecurity budgets increased from 6.8% in 2017 to 7.5% in 2019 (measured as a percentage of IT budget); every respondent either has established a cybersecurity program or is in the process of establishing a cybersecurity program; and 21 of 23 respondents develop software in-house.

The 2019 Survey will be published at:

Scott Russell, "2019 NSF Community Cybersecurity Benchmarking Survey Report,"  
<https://scholarworks.iu.edu/dspace/handle/2022/24912>

## 1.8 Presentations

Our outreach efforts, both to educate the community on cybersecurity for science and raise awareness of our services, included the following presentations. A list of presentations and slides presented may be found at <https://trustedci.org/presentations/>

- Terry Fleury, Ryan Kiser, and Jeremy Sampson. NEON & CI-CoE Pilot: Identity Management, a Story. 2019 NSF Cybersecurity Summit, October 2019.  
Slides: <http://bit.ly/2lvM39Z>
- Jim Basney, Terry Fleury, and Charles Nguyen. Risk Assessment Panel. 2019 NSF Cybersecurity Summit, October 2019.  
Slides: <http://bit.ly/38m8SZc>
- Von Welch. State of Trusted CI and NSF Trustworthy Cyberinfrastructure. 2019 NSF Cybersecurity Summit, October 2019.  
Slides:  
[https://figshare.com/articles/State\\_of\\_Trusted\\_CI\\_and\\_NSF\\_Trustworthy\\_Cyberinfrastructure/10079756/1](https://figshare.com/articles/State_of_Trusted_CI_and_NSF_Trustworthy_Cyberinfrastructure/10079756/1)
- Dana Brunson and Von Welch. Assuring Research Across the Quilt. The Quilt 2019 Fall Member Meeting, September 2019.  
Slides: [https://figshare.com/articles/Assuring\\_Research\\_Across\\_the\\_Quilt/9907493/1](https://figshare.com/articles/Assuring_Research_Across_the_Quilt/9907493/1)
- Von Welch. I Cut, You Choose: How to Share a Service? 2019 NSF Large Facilities CI Workshop panel on Shared CI Services: Opportunities and Challenges, September 2019.  
Slides:  
[https://figshare.com/articles/I\\_Cut\\_You\\_Choose\\_How\\_to\\_Share\\_a\\_Service\\_/9863846/1](https://figshare.com/articles/I_Cut_You_Choose_How_to_Share_a_Service_/9863846/1)
- Scott Russell. NCSA Cybersecurity and Networking Division Speaker Series. Learning Security's First Principles with the Super Mario Bros.  
Video: [https://www.youtube.com/watch?v=W9M\\_W-s6BsU](https://www.youtube.com/watch?v=W9M_W-s6BsU)  
Slides: <https://www.ideals.illinois.edu/handle/2142/105428>

- Florence Hudson. TIPSS (Trust, Identity, Privacy, Protection, Safety, Security) for Enabling & Securing Our Increasingly Connected World. Securing Research Data: A Workshop on Emerging Practices in Computation and Storage for Sensitive Data. August 2019.  
Slides: <https://ucsd-prp.gitlab.io/events/workshop-2019-srd/>
- Jim Basney. Trusted CI PEARC19 paper, Trusted CI Experiences in Cybersecurity and Service to Open Science. July 2019.  
Slides: <https://www.ideals.illinois.edu/handle/2142/104693>
- Jim Basney, et al. Trusted CI PEARC19 workshop. July 2019  
Slides: <https://www.ideals.illinois.edu/handle/2142/104693>
- Daniel Crawford, Ewa Deelman, Von Welch, Frank Wuerthwein, Mike Zentner and Jason Zurawski. Community Engagement at Scale: NSF Centers of Expertise. Panel at PEARC19, July 2019.  
Slides:  
[https://figshare.com/articles/Community\\_Engagement\\_at\\_Scale\\_NSF\\_Centers\\_of\\_Expertise/9177923](https://figshare.com/articles/Community_Engagement_at_Scale_NSF_Centers_of_Expertise/9177923)
- Von Welch. A 5-year Vision for an NSF Cybersecurity Ecosystem. PEARC19, July 2019.  
Slides:  
[https://figshare.com/articles/A\\_5-year\\_Vision\\_for\\_an\\_NSF\\_Cybersecurity\\_Ecosystem/9177920](https://figshare.com/articles/A_5-year_Vision_for_an_NSF_Cybersecurity_Ecosystem/9177920)
- Von Welch. Science and Networks and Cybersecurity. Training Workshop for Network Engineers and Educators on Tools and Protocols for High-Speed Networks, July 2019.  
Slides:  
[https://figshare.com/articles/Science\\_and\\_Networks\\_and\\_Cybersecurity/8984093](https://figshare.com/articles/Science_and_Networks_and_Cybersecurity/8984093)
- Von Welch. Trusted CI: The NSF Cybersecurity Center of Excellence. Briefing to the KINBER Cybersecurity Working Group, June 2019.  
Slides:  
[https://figshare.com/articles/Trusted\\_CI\\_The\\_NSF\\_Cybersecurity\\_Center\\_of\\_Excellence/8330210](https://figshare.com/articles/Trusted_CI_The_NSF_Cybersecurity_Center_of_Excellence/8330210)
- Ewa Deelman, Victoria Stodden, Michela Taufer and Von Welch. Initial Thoughts on Cybersecurity And Reproducibility. 2nd International Workshop on Practical Reproducible Evaluation of Computer Systems (P-RECS19), June 2019.  
Slides:  
[https://figshare.com/articles/Initial\\_Thoughts\\_on\\_Cybersecurity\\_And\\_Reproducibility/8316836/1](https://figshare.com/articles/Initial_Thoughts_on_Cybersecurity_And_Reproducibility/8316836/1)  
Paper: <https://dl.acm.org/citation.cfm?doid=3322790.3330593>
- Susan Sons and Von Welch. NSF Resources for Research Cybersecurity: Trusted CI and ResearchSOC. Cyberinfrastructure Brown Bag, June 2019.

Slides:

[https://figshare.com/articles/NSF\\_Resources\\_for\\_Research\\_Cybersecurity\\_Trusted\\_CI\\_and\\_ResearchSOC/8285783](https://figshare.com/articles/NSF_Resources_for_Research_Cybersecurity_Trusted_CI_and_ResearchSOC/8285783)

- Kay Avila, Bob Cowles, and Craig Jackson. A Practical Cybersecurity Framework for Open Science Projects and Facilities. Presented to the 2019 Great Plains Network All Hands Meeting. May 2019.

Slides: <https://www.ideals.illinois.edu/handle/2142/103989>

- Ryan Kiser and Anurag Shankar. Building a NIST Risk Management Framework for HIPAA, CUI, and FISMA. Presented to the 2019 Great Plains Network All Hands Meeting. May 2019.

Slides: <https://www.ideals.illinois.edu/handle/2142/103990>

- Von Welch. Cybersecurity to Enable Science: Hindsight and Vision from the NSF Cybersecurity Center of Excellence. Presented at NCSA, May 2019.

Video: <https://www.youtube.com/watch?v=3Hqat79hL5I>

Slides: <https://www.ideals.illinois.edu/handle/2142/103985>

- Von Welch. FAIR in an unfair world: Cybersecurity, data breaches, data integrity, and open science. Keynote at the International Symposium on Grids & Clouds 2019 (ISGC 2019), April 2019.

Slides:

[https://figshare.com/articles/FAIR\\_in\\_an\\_unfair\\_world\\_Cybersecurity\\_data\\_breaches\\_data\\_integrity\\_and\\_open\\_science/7949675](https://figshare.com/articles/FAIR_in_an_unfair_world_Cybersecurity_data_breaches_data_integrity_and_open_science/7949675)

- Bart Miller and Elisa Heymann led a session called Maritime Software Security through In-Depth Assessment, Education and Recovery at the 3rd NATO NMIOTC Cyber Security Conference in Crete, Greece, April 2019.

- Von Welch, Jim Basney and Bob Cowles. A Cybersecurity Framework for Open Science: Motivations and Requirements Discussion. 2019 ISGC Security Workshop, March 2019.

Slides:

[https://figshare.com/articles/A\\_Cybersecurity\\_Framework\\_for\\_Open\\_Science\\_Motivations\\_and\\_Requirements\\_Discussion/7930331](https://figshare.com/articles/A_Cybersecurity_Framework_for_Open_Science_Motivations_and_Requirements_Discussion/7930331)

- Mike Corn and Von Welch. Cybersecurity to Enable Science: Hindsight and Vision from the NSF Cybersecurity Center of Excellence. CENIC 2019, March 2019.

Slides:

[https://figshare.com/articles/Cybersecurity\\_to\\_Enable\\_Science\\_Hindsight\\_and\\_Vision\\_from\\_the\\_NSF\\_Cybersecurity\\_Center\\_of\\_Excellence/7871786](https://figshare.com/articles/Cybersecurity_to_Enable_Science_Hindsight_and_Vision_from_the_NSF_Cybersecurity_Center_of_Excellence/7871786)

- Jim Basney, Mike Corn and Von Welch. Strategies for Research Cybersecurity and Compliance from the Lab. 2019 Internet2 Global Summit, March 2019.

Slides:

[https://figshare.com/articles/Strategies\\_for\\_Research\\_Cybersecurity\\_and\\_Compliance\\_from\\_the\\_Lab/7871777](https://figshare.com/articles/Strategies_for_Research_Cybersecurity_and_Compliance_from_the_Lab/7871777)

- Von Welch. Cybersecurity for Open Science. 2019 Internet2 Global Summit Executive Track, March 2019.  
Slides: [https://figshare.com/articles/Cybersecurity\\_for\\_Open\\_Science/7864745](https://figshare.com/articles/Cybersecurity_for_Open_Science/7864745)
- Von Welch. Cybersecurity for Trustworthy Science: The NSF Cybersecurity Center of Excellence. SIAM CSE19 Broader Engagement Mini-symposium on Securing Extreme-Scale Scientific Computing, February 2019.  
Slides:  
[https://figshare.com/articles/Cybersecurity\\_for\\_Trustworthy\\_Science\\_The\\_NSF\\_Cybersecurity\\_Center\\_of\\_Excellence/7929131](https://figshare.com/articles/Cybersecurity_for_Trustworthy_Science_The_NSF_Cybersecurity_Center_of_Excellence/7929131)
- Jim Basney. Trusted CI's approach to security for open science projects, 13th FIM4R Workshop, February 2019  
Slides: <https://www.ideals.illinois.edu/handle/2142/102973>

## 1.9 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 secure our science and our country. Successful TTP can be via commercialization, industry partnerships, start-ups, open source, or deployment in higher ed, NSF projects, or government. 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 engagements, 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.

In 2019, we honed our focus on the specific cybersecurity and TTP needs and gaps enunciated in the TTP cybersecurity and cyberinfrastructure expert interviews conducted in 2H2018. These interviews with NSF large facilities, academia, research computing, and industry identified focus areas for the 2019 TTP program.

Top cybersecurity needs / gaps identified in the community interviews were:

- Artificial intelligence / machine learning for cybersecurity including log analysis, intrusion detection, data reduction, insider/outsider threat, SW verification
- Global distributed federated identity management - students, researchers, patients, devices, clients, employees – to ease collaboration and reduce risk
- Internet of things / cyber physical systems (IOT/CPS) privacy and security risk mitigation
- Security and privacy education and workforce development

The top TTP needs / gaps identified were:

- Include business partners with researchers and practitioners in the TTP collaboration, e.g., entrepreneurs, industry, VCs
- Add co-creation, the collaborative development between researchers and practitioners, to the TTP workshop to clarify practitioner needs, determine the research fit for the needs, and develop steps to transition research to practice collaboratively for researchers working with practitioners
- Enable earlier collaboration between researchers and practitioners so software and solutions are developed with operations in mind
- Provide testbeds to test research before deployment (for instance via ResearchSOC)

We analyzed over 1000 NSF awards to identify research/researchers to fill the expert-defined gaps, including 903 SaTC awards, 99 TTP awards, and 100+ CICI PI meeting presentations.

To fulfill our goal to address the cybersecurity and TTP needs identified in the expert interviews, including increasing researcher and practitioner collaboration and matchmaking to enable TTP, we held the 2019 cybersecurity TTP and Co-creation workshop<sup>18</sup> on June 19th in Chicago. Academia, tech transfer and industry collaboration was further supported by workshop sponsorship in the form of Microsoft hosting the workshop at their Aon Center location in Chicago, with breakfast and lunch sponsored by the IURTC (Indiana University Research and Technology Corp.), Box, and Trusted CI. The workshop had 59 attendees, nearly double the initial goal of 30 attendees. There were 33 presenters consisting of 15 academic researchers, 4 industry practitioners in cybersecurity including large industry and entrepreneurs, 2 higher ed CIOs, a large facility cyberinfrastructure leader, a regional network, plus 10 posters presented by 9 students and research faculty. Results were excellent, with 162 requests for one-on-one matchmaking connections between participants, and 100% excellent or good (4 or 5 on a scale of 1 to 5) overall experience ratings. We received 5 offers to host subsequent workshops in Austin (National Instruments), San Francisco (Box), Philadelphia (Temple University Researcher), North Carolina (UNC Charlotte Researcher), and West Virginia (Marshall University CIO).

The TTP workshop consisted of five collaborative integrated researcher + practitioner panels, each beginning with opening remarks by higher ed and industry cybersecurity practitioners detailing cybersecurity challenges they face, then 15 minute TED-style talks by researchers, culminating in co-creation discussions of how we can move the research into practice. The topics for the integrated panels of practitioners and researchers were based on the results of our 2018 cybersecurity needs and gaps survey, focused on these needs and gaps:

- Artificial intelligence / machine learning for cybersecurity

---

<sup>18</sup> <https://trustedci.org/2019-ttp-workshop>

- Cybersecurity risk mitigation in data, cloud and cyberinfrastructure
- Human factors in cybersecurity including reducing phishing attacks
- Internet of things / cyber-physical systems / networking cybersecurity
- TTP success stories, including identity management and intrusion detection

The 10 posters presented by 9 students and research faculty, some supporting specific presentations by their professors on the panels, is a step in enabling workforce development and building of the pipeline of future cybersecurity researchers and leaders. A robust Twitter and email campaign engaging underrepresented groups in cybersecurity and STEM led to 30% of attendees being women, higher than current estimates of the female percentage of the cybersecurity workforce.



**Figure 4. TTP Workshop in Chicago**

Additional actions taken to address the community recommendations for TTP in 2019 were:

- Added a “Co-creation” theme to the TTP workshop to encourage active clarification of practitioner needs.
- Orchestrated one on one matchmaking between researchers and practitioners in industry, government, not for profits, academia before, during and after the workshop.
- Hosted a TTP researcher presentation on the February, 25 2019 Trusted CI Webinar in one of the TTP focus areas, AI/ML for Cybersecurity.

Separately, at the EDUCAUSE Security Professionals Conference, Florence Hudson hosted a BOF regarding TTP on May 13 called “Cybersecurity Needs and Partnering with Researchers to Fill the Gaps” with Helen Patton, The Ohio State University CISO. There were 10 attendees. The key input was to consider how higher ed CISOs could provide cybersecurity data to a shared and secured data lake to be used by cybersecurity researchers, who could then provide value back to the higher education cybersecurity data providers, potentially in partnership with ResearchSOC.

The TTP matchmaking efforts prior to our 2019 TTP workshop resulted in the identification of three new NSF TTP success stories, CILogon (NCSA/UIUC), SecureMPC (Boston University) and Human factors in Cybersecurity (Temple University), which joined the well known success of Bro (ICSI), in being highlighted in the workshop to inspire future TTP success.

From the workshop and other 2019 TTP efforts, we identified the following five examples of ongoing NSF cybersecurity TTP, with potential users. We expect to shepherd and follow these and other efforts in 2020 to identify further customers and develop lessons learned to disseminate to the broader NSF TTP community.

- Dr. Shantanu Chakrabartty, Washington University – St Louis, research for IOT/CPS security - collaborating with AT&T, National Instruments (joint SaTC TTP proposal), MVP start-up plans
- Dr. Jay Yang, Rochester Institute of Technology, research for AI/ML for cybersecurity, collaborating with Academia (IU, UT Austin, Marshall University, UCSD, Duke), and a National Lab
- Dr. Miroslav Pajic, Duke University, research in Cyber Physical Systems (CPS), collaborating with National Instruments
- Dr. Jean Camp, Indiana University, research in AI/ML, collaborating with a National Lab
- Richard Biever, research for honeypot collaborative cybersecurity called STINGAR, collaborating with other researchers including Jay Yang at RIT and universities deploying STINGAR, and interested in new potential STINGAR users, in collaboration with ResearchSOC

## 1.10 Social Media Impact

This section covers our social media impact, broken down by Twitter impressions<sup>19</sup>, blog page views, and unique website visitors. Table 2 shows the stats collected in 2019. The last row lists the stats from 2018 and demonstrates a clear growth in our social media impact compared to last year.

---

<sup>19</sup> Number of times users saw a Tweet on Twitter

**Table 2. Social media impact 1Q2019.**

<b>Date</b>	<b>Twitter Impressions</b>	<b>Blog Page Views</b>	<b>Unique Website Visitors</b>
Jan.	11.5K	2.1K	.7K
Feb.	10.7K	2.5K	1K
Mar.	10.3K	2.4K	1.2K
Apr.	11.9K	2.9K	1K
May	9K	2.5K	1.7K
Jun.	10K	2.7K	1.2K
Jul.	11.1K	2.1K	1.6K
Aug.	10.9K	2.5K	1.4K
Sept.	64.2K	2.9K	1.2K
Oct.	31K	4K	1.8K
Nov.	6.8K	3.6K	1.1K
Dec.	1.7K	2.6K	.5K
<b>Total 2019</b>	<b>189.1K</b>	<b>32.8K</b>	<b>14.3K</b>
Total 2018 (for comparison)	82.4K	18.5K	7.7K

## 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<sup>20</sup> (OSCRP) is a living and published<sup>21</sup> document designed to help principal investigators and their supporting information technology professionals assess cybersecurity risks related to open science projects. The initial version is the product of Trusted CI in collaboration with LBNL/ESnet, specifically Sean Peisert, who has since joined Trusted CI, Michael Dopheide, and research and education community leaders, including: RuthAnne Bevier (Caltech), Rich LeDuc (Northwestern), Pascal Meunier (HUBzero), Steve Schwab (ISI), and Karen Stocks (UCSD).

In 3Q and 4Q2019, Trusted CI conducted an investigation of data integrity issues due to natural faults and mechanical failures, including examining industry documentation, both experimental

<sup>20</sup> <https://trustedci.github.io/OSCRP/OSCRP.html>

<sup>21</sup> <https://scholarworks.iu.edu/dspace/handle/2022/21259>

and theoretical academic studies, and numerous in-depth conversations with a variety of scientific computing systems in the field. This too, included examining both individual science projects as well as international data repositories and computing centers. The scope of the investigation included components of individual computing systems, as well as networks, sensors, USB storage, and cloud computing, and also examined integrity issues in “extreme” (e.g., high radiation) environments. The result of this effort will itself be distributed as a standalone report in late 2019, serving as the basis for a community discussion regarding data integrity, and as an input to the 2020 Trusted CI challenge on data integrity. The report is available at this URL: <http://hdl.handle.net/2022/24910>

In terms of impact and knowledge transfer, we note the following:

In 1Q2019, the OSCRIP was promoted in NSF’s CICI solicitation (19-514)<sup>22</sup> as a suggested tool for applicants in the solicitation.

In October 2019, the OSCRIP was positively referenced in a peer-reviewed publication on security and privacy issues in academia:

- Leonie Maria Tanczer, Ronald J Deibert, Didier Bigo, M I Franklin, Lucas Melgaço, David Lyon, Becky Kazansky, Stefania Milan, Online Surveillance, Censorship, and Encryption in Academia, International Studies Perspectives, ekz016, <https://doi.org/10.1093/isp/ekz016>

## 2.2 Situational Awareness / Cyberinfrastructure Vulnerabilities

The Cyberinfrastructure Vulnerabilities (CV) 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 freely available to all by subscribing to Trusted CI’s mailing lists.<sup>23</sup>

We monitor a number of sources for software vulnerabilities of interest, then determine which ones are of the most critical interest to the community. While it’s easy to identify issues that have piqued the public news cycle, we strive to alert on issues that affect the science CI community in particular. These are identified using the following criteria: the affected technology’s or software’s pervasiveness in the community; the technology’s or software’s importance to the community; type and severity of potential threat, e.g., remote code execution; the threat’s ability to be remotely triggered; the threat’s ability to affect critical core functions; and if mitigation is available. 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, the NSF supercomputing centers, and the

---

<sup>22</sup> [https://www.nsf.gov/pubs/2019/nsf19514/nsf19514.htm?WT.mc\\_id=USNSF\\_25&WT.mc\\_ev=click](https://www.nsf.gov/pubs/2019/nsf19514/nsf19514.htm?WT.mc_id=USNSF_25&WT.mc_ev=click)

<sup>23</sup> <https://trustedci.org/vulnerabilities/>

ResearchSOC on drafting and distributing alerts to minimize duplication of effort and maximize the benefit from community expertise.

Sources we monitor for possible threats to science CI include:

- OpenSSL, OpenSSH, and Globus project and security announcements
- US-CERT advisories<sup>24</sup>
- XSEDE announcements
- RHEL/EPEL advisories
- REN-ISAC Alerts and Advisories<sup>25</sup>
- 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 2019, we issued 25 cyberinfrastructure vulnerability alerts to 144 subscribers.<sup>26</sup> The 144 subscribers represents a 25% increase from 2018. Similarly, the 25 alerts in 2019 was a 36% increase from the previous year – this suggests either an inherent improvement in that security researchers are getting better at finding vulnerabilities and-or that more vulnerabilities are being introduced in systems, which is clearly a detriment to science.

As alluded to above, we coordinate with XSEDE and the ResearchSOC. The CV lead routinely participates in the XSEDE weekly Incident Response/Trust group security meetings and is a member of the ResearchSOC's ISO. The purpose is to get feedback on current vulnerabilities that are being reviewed and to determine relevance to the CI community. Finally, we also gained a new non-funded resource to participate in the CI Vulnerability program: Scott Sakai, Security Analyst at San Diego Supercomputing Center, has volunteered to help identify, assess and develop mitigations for vulnerabilities that affect the community.

## 2.3 Publications

Trusted CI produced the following publications in 2019:

- E. Deelman, V. Stodden, M. Taufer and V. Welch. "Initial Thoughts on Cybersecurity and Reproducibility. Proceedings of the 2nd International Workshop on Practical Reproducible Evaluation of Computer Systems (P-RECS'19), 2019."  
Paper: <https://doi.org/10.1145/3322790.3330593>.  
Slides: <https://doi.org/10.6084/m9.figshare.8316836.v1>
- A. Adams, K. Avila, J. Basney, D. Brunson, R. Cowles, J. Dopheide, T. Fleury, E. Heymann, F. Hudson, C. Jackson, R. Kiser, M. Krenz, J. Marsteller, B. Miller, S. Piesert, S. Russell, S.

---

<sup>24</sup> <https://www.us-cert.gov/ncas/current-activity>

<sup>25</sup> <https://www.ren-isac.net/public-resources/AlertsAdvisories.html>

<sup>26</sup> <https://list.iu.edu/sympa/arc/cv-announce-l>

Sons, V. Welch and J. Zage, “Trusted CI Experiences in Cybersecurity and Service to Open Science. PEARC'19: Practice and Experience in Advanced Research Computing, 2019.”

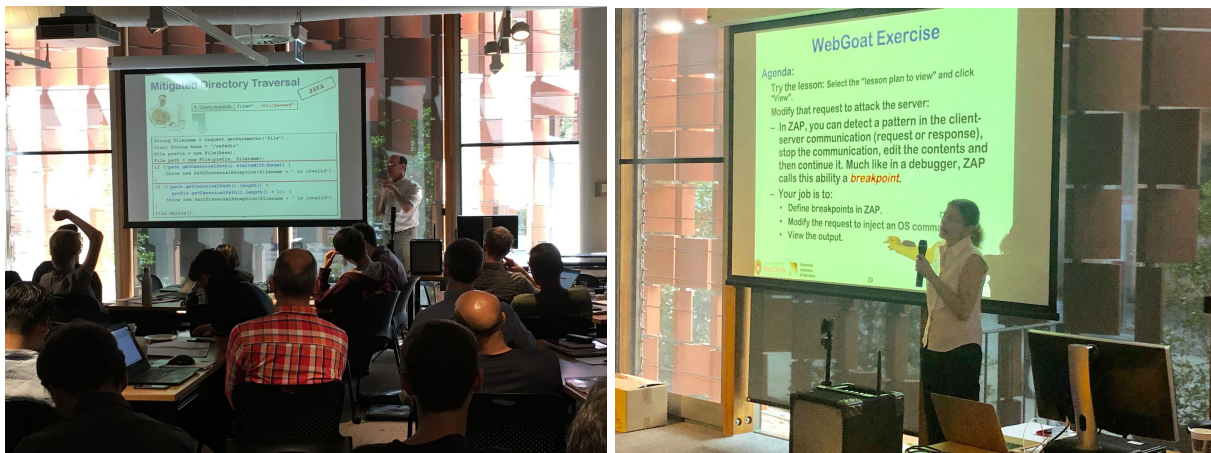
<https://doi.org/10.1145/3332186.3340601>

- (To be published in January 2020) Andrew Adams, Kay Avila, Kathy Benninger, Jeannette Dopheide, Mark Krenz, James Marsteller, and John Zage. Report of the 2019 NSF Cybersecurity Summit for Cyberinfrastructure and Large Facilities: <http://hdl.handle.net/2142/105533>
- Reinhard Gentz and Sean Peisert, “An Examination and Survey of Random Bit Flips and Scientific Computing,” December 2019. <http://hdl.handle.net/2022/24910>

## 2.4 Training

Besides training delivered at PEARC19 and the 2019 NSF Cybersecurity Summit, which is covered elsewhere in this report, Trusted CI delivered the following training in 2019:

- Bart Miller and Elisa Heymann taught a 8-hour tutorial on “Secure Coding Practices and Automated Assessment Tools”, at the University of Queensland, Brisbane, Australia, May 2019.



**Figure 5. Photos from the tutorial at the University of Queensland**

- Bart Miller and Elisa Heymann taught a 4-hour tutorial on “Secure Coding Practices and Automated Assessment Tools”, at the University of Iowa, Iowa City, Iowa, September 2019.



**Figure 6. Photos from the tutorial at the University of Iowa.**

- Bart Miller and Elisa Heymann taught a half-day tutorial on “Secure Coding Practices and Automated Assessment Tools”, at Gateways’19, San Diego, California, September 2019.



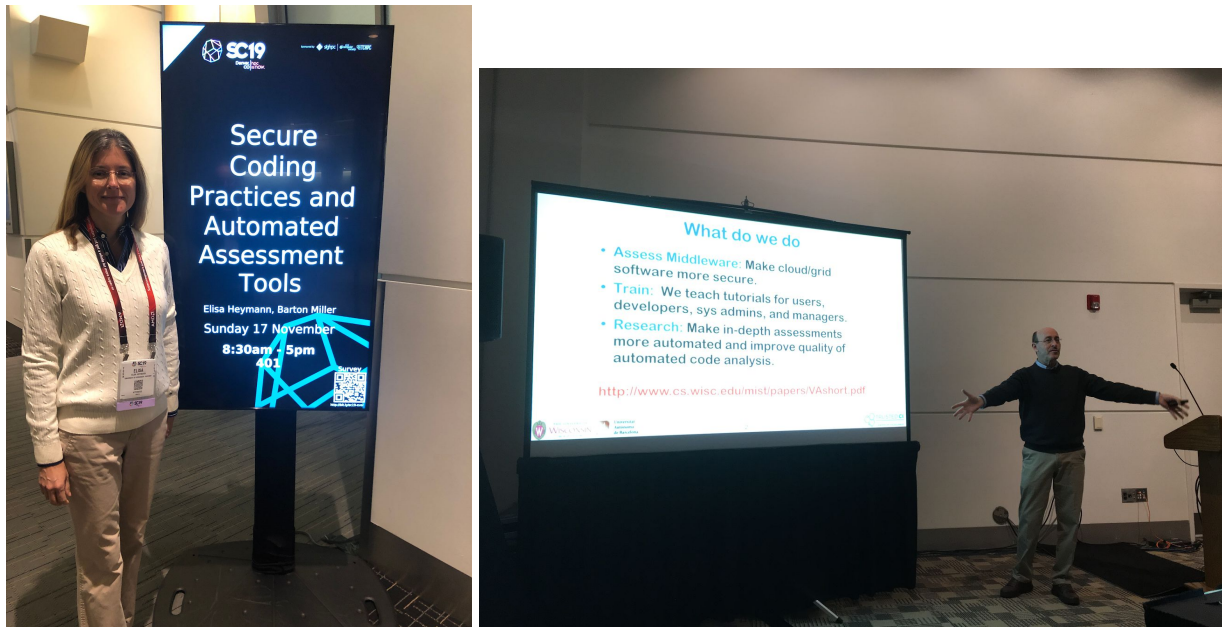
**Figure 7. Photos from the tutorial at Gateways’19**

- Bart Miller and Elisa Heymann taught a half-day tutorial on “Secure Coding Practices and Automated Assessment Tools”, at Cal Poly Pomona, SFSCon, Pomona, California, September 2019.



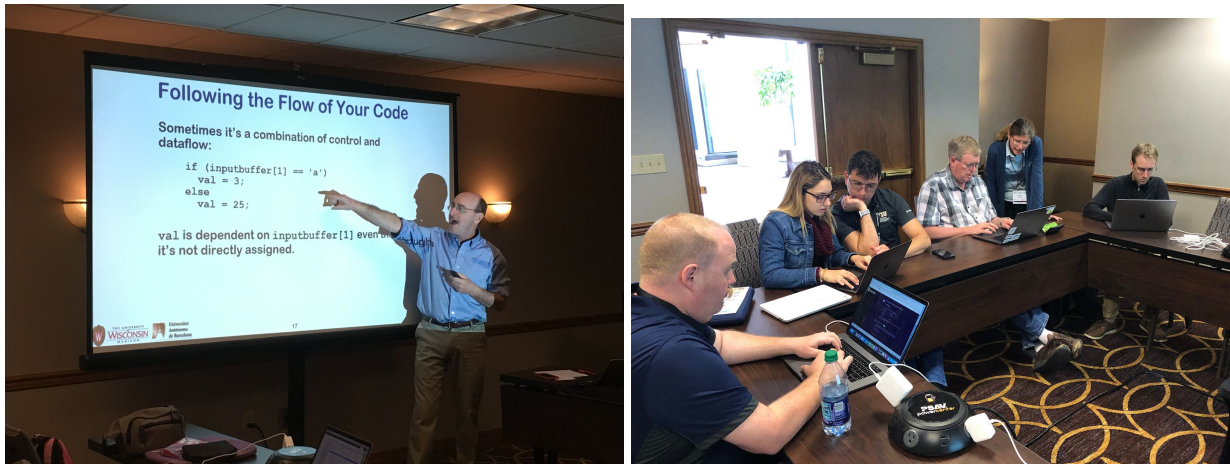
**Figure 8. Photos from the tutorial at SFSCon, at Cal Poly Pomona.**

- Bart Miller and Elisa Heymann taught a half-day tutorial on “Web Security and Automated Assessment Tools”, at the NSF Cybersecurity Summit, San Diego, California, October 2019.
- Bart Miller and Elisa Heymann taught a full-day tutorial on “Secure Coding Practices and Automated Assessment Tools”, at SuperComputing’19, Denver, Colorado, November 2019.



**Figure 9. Photos from the tutorial at SuperComputing’19**

- Bart Miller and Elisa Heymann taught a full-day tutorial on “Secure Coding Practices and Automated Assessment Tools”, at Internet2 Technology Exchange, New Orleans, Louisiana, December 2019.



**Figure 10. Photos from the tutorial at Technology Exchange**

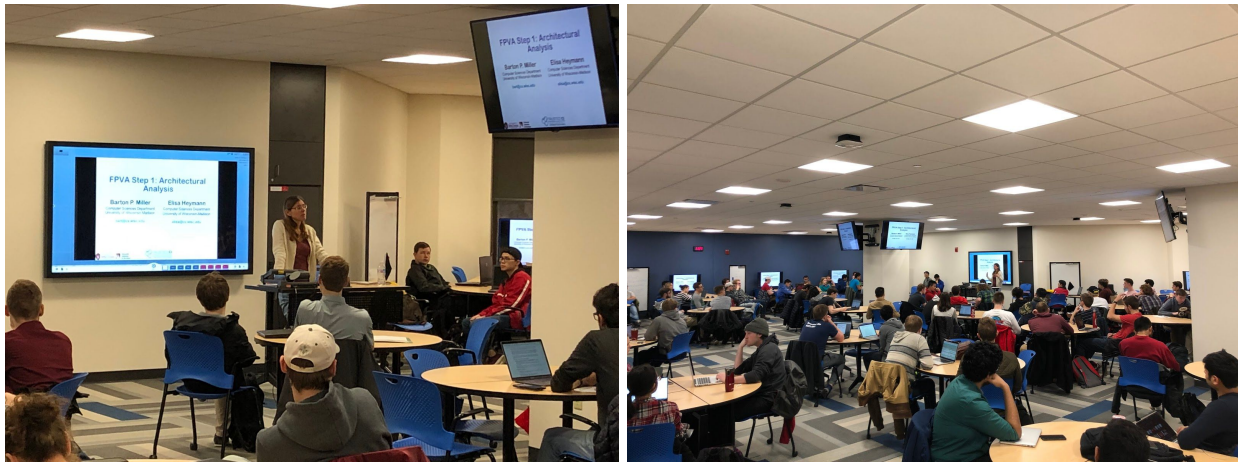
Trusted CI led three workshops at the 2019 Great Plains Network All Hands Meeting in May:

- Ryan Kiser and Anurag Shankar led a workshop called Building a NIST Risk Management Framework for HIPAA, CUI, and FISMA at the 2019 Great Plains Network All Hands Meeting in May. The slides from this workshop are located here: <http://hdl.handle.net/2142/103990>.
- In addition, Ishan Abhinit and Mark Krenz led a Security Log Analysis workshop. The slides from this workshop are located here: <http://hdl.handle.net/2022/23213>.
- Lastly, Kay Avila, Bob Cowles, and Craig Jackson led A Practical Cybersecurity Framework for Open Science Projects and Facilities, for which the slides can be found here: <http://hdl.handle.net/2142/103989>

## 2.5 Software Security Course Development

In the Spring 2019 semester (starting January 2019) Bart Miller and Elisa Heymann taught a 3-credit course, *Introduction to Software Security* (CS639), at the University of Wisconsin-Madison to 120 students (mostly senior Computer Science and Computer Engineering majors). This course was based on the video modules and text chapters prepared under the Trusted CI funding by Miller and Heymann (material available online<sup>27</sup>). The course followed the flipped-classroom model, which means that class time is used for active learning with activities such as group discussions and problem-solving.

<sup>27</sup> <http://research.cs.wisc.edu/mist/SoftwareSecurityCourse/>



**Figure 11. Pictures from CS639 at the University of Wisconsin-Madison**

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 area delivered in virtual machines<sup>28</sup>. In addition, each week includes a quiz to assess the work performed on the hands-on exercises.

The topic covered by CS 639 are:

- Introductory concepts.
- Thinking like an attacker.
- Secure design principles.
- Security problems with Pointers and Strings.
- Numeric Errors.
- Security problems with Serialization.
- Security problems with Exceptions.
- Directory traversal.
- Injections (Introduction to injections, SQL injections, XML injection, Command injections, Code injections, JSONP injections).
- Web attacks (XSS, CSRF, Session management, OpenRedirect).
- Security for mobile.
- In-depth vulnerability assessments with FPVA.
- Automated assessment tools and the SWAMP.
- Fuzz testing.
- System defenses (address space layout randomization, heap guards, stack canaries, control flow integrity checking).

<sup>28</sup> <https://research.cs.wisc.edu/mist/SoftwareSecurityCourse/Exercises/security-exercises.ova>

The class used their self-contained hands-on exercises for Exceptions, Serialization, Directory traversal, SQL Injection, Command Injection, XML and JSONP injections, XSS, CSRF, mobile, and FPVA.



**Figure 12. Pictures from CS639 at the University of Wisconsin-Madison**

Feedback from the students was mostly positive, and we also received suggestions to improve future editions of the course. It is challenging to teach students with widely varying background courses and interests, so some students found the course easy while others found it challenging. We provided exercises for extra credit to help with that situation.

## 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 2019, the Framework was one of our major strategic initiatives. In 1Q2019, we finalized major architectural decisions around the Framework Implementation Guide (FIG) for scientific CI and prepared for substantial community engagement.

We provisionally finalized the language of the 16 "Musts" that form the core requirements of the Framework, their descriptions to help users unpack their meaning, and the primary audience for the first Framework Implementation Guide (i.e., research infrastructure operators). To socialize and receive feedback on our plans for the Framework, we presented an overview of our plans at the International Symposium on Grids and Clouds (ISGC) in Taiwan, WISE in Lithuania, Great Plains Network (GPN) event in Kansas City, the April Large Facility

Security Team meeting, the Trusted CI webinar series, and the 2019 NSF Summit. We recruited an advisory review group representing a cross-section of the community for our Framework Implementation Guide development effort as well as a set of early adopters. The advisory review group currently has 14 members from NSF major facilities, other NSF projects, ESnet, and institutions of higher education. We actively utilized the Framework in our engagement with the Scripps Institution of Oceanography.

## 2.7 Secure Software Engineering Guide

The Secure Software Engineering Guide was funded by a supplement from NSF to bolster Trusted CI software security efforts. Prior to this effort, no agreed-to or widely implemented software quality or assurance standards exist for scientific software and cyberinfrastructure. 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 will 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”.

Rough drafts are available (live, as edits are added) at <https://sweguide.trustedci.org> and the final publication is expected by the end of 2019, including additions made under a collaboration with the Collaborative Research: EAGER: Exploring and Advancing the State of the Art in Robust Science in Gravitational Wave Physics project (NSF award 1823405). The EAGER project funded content additions specifically addressing reproducibility needs of these small software components that greatly impact scientific projects’ data processing, and the engineering practices that mitigate threats to reproducibility.

## 2.8 Broader Impacts

Examples of Trusted CI’s broader impacts in 2019 are:

- Trusted CI is now listed as a resource on the Women in Cybersecurity website<sup>29</sup>.
- The cloudperm software discussed in section 1.4 is being utilized in two projects outside of Trusted CI: the Science Gateway Community Institute<sup>30</sup> and the PACT project.

---

<sup>29</sup> <https://www.wicys.org/other-security-resources>

<sup>30</sup> <https://www.sciencegateways.org/>

- Trusted CI and ResearchSOC are now both partners with the EDUCAUSE Higher Education Information Security Council (HEISC)<sup>31</sup>. This partnership means additional dissemination of Trusted CI activities and products to the HEISC community, which represents a significant set of stakeholders: information security professionals across higher education.
- To educate legislators and policy makers on cybersecurity for scientific research, Trusted CI Director Von Welch presented at the CNSF 25th Annual Exhibition and Reception in the Rayburn House Office Building<sup>32</sup>, briefed Representative Jim Banks, and helped federal liaisons at IU and EDUCAUSE understand science ramifications of pending legislation.
- Trusted CI Director Von Welch was named IU's first Executive Director for Cybersecurity Innovation<sup>33</sup>, recognizing his impact on both cybersecurity research and cybersecurity for research, and giving him a prominent role in these areas at IU and a platform to better understand these areas to benefit Trusted CI.
- IU CACR applied expertise gained in leading Trusted CI to working with the Indiana Secretary of State to protect Indiana's 2020 elections<sup>34</sup>, its work with the Department of Defense<sup>35</sup>, and in its CyberCamps teaching cybersecurity basics to high schoolers and non-STEM undergraduates (the latter in collaboration with IU's Center of Excellence for Women and Technology)<sup>36</sup>.
- Through a student affiliate program with the Indiana University Maurer School of Law, law students gain experience working with CACR's on-staff legal experts, including work on the Trusted CI Law and Policy Insights project described in Section 2.10.
- Bart Miller and Elisa Heymann taught a full day tutorial (8 hours) in Secure Programming and Automated Assessment Tools, at (and funded by) the University of Queensland, in Brisbane, Australia, in May 2019. There were 52 attendees from the Australian defense establishment, Australian CERT, Boeing Australia, members of the University of Queensland academic community, and a variety of other local companies.

## 2.9 Fellows Program

The Trusted CI Open Science Cybersecurity Program developed and launched the Fellows program in 1Q2019<sup>37</sup>. The application and criteria for selection were developed and

---

<sup>31</sup> <https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/about-heisc>

<sup>32</sup> [https://cnsf.us/exhibitions/CNSF\\_Program2019\\_v3\\_040519\\_Final.pdf](https://cnsf.us/exhibitions/CNSF_Program2019_v3_040519_Final.pdf)

<sup>33</sup> <https://news.iu.edu/stories/2019/05/iu/releases/30-von-welch-executive-director-cybersecurity.html>

<sup>34</sup> <https://indianavoters.in.gov/MVPHome/ElectionSecurity>

<sup>35</sup>

<https://www.navsea.navy.mil/Media/News/Article/1637336/nswc-crane-and-indiana-universitys-center-for-applied-cybersecurity-research-ad/>

<sup>36</sup> <https://cacr.iu.edu/events/security-matters-cybercamps.html>

<sup>37</sup> <https://trustedci.org/fellows>

disseminated broadly in February with Applications due on March 13th. Twenty-two applications were received, reviewed, and the six were accepted.

The Trusted CI Open Science Cybersecurity Program announced its inaugural cohort of individuals in mid-April and includes: Shafaq Chaudhry, University of Central Florida; Matias Carrasco Kin, NCSA; Gabriella Perez, University of Iowa; Aunshul Rege, Temple University; Chrysafis Vogiatzis, North Carolina A&T State University; and S. Jay Yang, Rochester Institute of Technology.

The Virtual Institute commenced its weekly Zoom sessions on May 14th with introductions and an overview of Trusted CI. Virtual Institute Sessions included: “Components of a cybersecurity program,” by Craig Jackson (IU); “Introduction to cybersecurity, what is the goal of cybersecurity for science, how is it different?” by Von Welch (IU); “(Ex-)CISO Perspective on Research Cybersecurity,” by Tom Barton (U Chicago); “Baseline Controls,” by Bob Cowles; “Cybersecurity Budgeting,” by Scott Russell (IU); “European Cybersecurity Perspective,” by David Kelsey (STFC, UK); “Swift & Reasonable Action: A Higher Ed CISO’s Perspective,” by Andrew Korty (IU); “Firewalls,” Kay Avila (NCSA); “ResearchSOC and Incident Response,” by Susan Sons (IU); “Trusted CI Cybersecurity Program,” by Jim Marsteller (Penn State); “ScienceDMZ Architecture and Security,” by Nick Buraglio (ESNet); “Hacks and Counter-Hacks: How the Bad Guys Think about Your Code and Some Defensive Techniques,” by Bart Miller and Elisa Heymann (U. Wisconsin); “Identity and Access Management (IAM) for Research Collaborations,” by Jim Basney (NCSA); “Reproducibility and Replicability in Cyberinfrastructure Systems,” by Victoria Stodden (UIUC); “Cybersecurity - A service provider perspective,” Erik Deumens (U Florida); “NSF talk to Trusted CI Fellows,” by Kevin Thompson (NSF); “Cyber Security & Open Science,” by Tim Hudson (NEON); and “Industrial Control System Security,” by Phil Salkie (Jenarlah Industrial Automation).

The Fellows served on a panel at PEARC19 within the Trusted CI workshop as well as on a plenary panel session at the 2019 NSF Cybersecurity Summit.

In the weeks following the conclusion of the Virtual Institute, Trusted CI staff and Fellows have continued to meet on a weekly basis. During these meetings the Fellows each presented their work and discussed how they are applying what they have learned from the Fellows program in their communities. Additionally, the 2019 Fellows have provided feedback on the program and have indicated interest in further participation, such as mentoring the next cohort of fellows, participating in the design of the Virtual Institute, and participating in other Trusted CI endeavors.

During the Trusted CI Fellows Panel at the NSF Cybersecurity Summit, the Call for Applications for the 2020 cohort of fellows was released with applications due Jan. 17, 2020. A webinar about the Fellows program and featuring the 2019 Fellows was held Tuesday, Dec. 17, 2019.

## 2.10 Law and Policy Insights

In 3Q2018, Trusted CI initiated the Law and Policy Insights effort in response to the ongoing need for clarity in the community regarding emerging legal and regulatory issues. In recent years, issues arising from laws and regulations have been a recurring source of concern and confusion in the community, most notably the requirements to protect Controlled Unclassified Information (CUI) by adhering to NIST SP 800-171 and the European Union’s General Data Protection Regulation (GDPR). When these issues emerged, Trusted CI dynamically responded by using our on-staff legal experts to provide generalized guidance to the community on what these laws mean and how they might impact the science community. The success and positive feedback from these dynamically generated guidance materials ultimately led to the creation of the “Law and Policy Insights” project, which will provide this type of analysis on a more consistent basis.

Previous guidance materials include:

- Blog Post on CUI and NIST SP 800-171 for the Trusted CI Blog
- Presentation on NIST SP 800-171, NIST RMF, and NIST CSF at the 2017 NSF Cybersecurity Summit
- Presentation on GDPR on the Large Facilities Security Team conference call in April 2018
- Presentation on GDPR for the Trusted CI Webinar series in May 2018
- Training session on GDPR at the 2018 NSF Cybersecurity Summit
- Presentation on GDPR at the Fall 2018 CEWIT Cyber camp

In Fall 2018, CACR established a student affiliate program with the Indiana University Maurer School of Law, wherein law students would gain experience working with CACR’s on-staff legal experts, including work on the Trusted CI Law and Policy Insights project. In Spring 2019, we had two law student affiliates research two areas of interest to the community: the recent California Consumer Privacy Act (CCPA) and export control laws, particularly as applied to software. These research efforts produced two memorandum delivered by the project lead and one presentation on export control law during a “Brown Bag” lunch hosted at CACR.

In Summer 2019, Trusted CI became aware of the Department of Defense’s Cybersecurity Maturity Model Certification (CMMC), an in-development cybersecurity framework that is likely to impact at least a subset of the NSF science community. The Law and Policy project dynamically addressed this emergent issue, beginning with the development of memoranda summarizing and analyzing the facts as currently known, brief status updates on CMMC developments circulated through email, and ultimately creating a blog post on the Trusted CI blog. The Law and Policy project will continue to address this emergent issue in 2020.

Additionally, in Fall 2019 the project lead presented a webinar for the Webinar on GDPR one year later, the California Consumer Protection Act (CCPA), and the future of international privacy laws. The presentation was attended by 19 attendees, and the feedback received after the presentation was part of the basis for the creation of more in-depth guidance materials on particular topics in 2020.

### 3 One-on-One Collaborations: Engagements

This section covers our engagements, that is, six-month collaborations selected through a competitive application process with specific NSF projects and supporting organizations to tackle their specific challenges with cybersecurity in the support of NSF science.

#### 3.1 Engagement Applications

In 1Q2019, we opened and publicized a call for applications for engagements to be executed in the second half of 2019<sup>38</sup>. In 2Q2019, we received 11 applications and selected the following engagements:

- Globus (various awards)
- Services Layer at the Edge (SLATE) (Award #1724821)
- US Academic Research Fleet (US ARF) (NSF Division of Ocean Sciences, various awards)
- University NAVSTAR Consortium (UNAVCO)/Geodesy Advancing Geosciences and EarthScope (GAGE) (Award #1724794)

It is interesting to note that, when we reviewed the engagement applications received from US ARF and UNAVCO/GAGE, we were unsatisfied with the level of cybersecurity commitment indicated. We have found that insufficient commitment can mean that our recommendations can go unimplemented. We requested both projects demonstrate strong management commitment, including designating a chief information security officer. In consultation with NSF, US ARF was able to satisfy our request and we are proceeding with our engagement. Resource constraints prevented UNAVCO/GAGE from meeting our request and we scaled down our engagement to a brief two-week “cybercheckup” to guide and hopefully motivate their increased investment in cybersecurity.

In 3Q2019, we opened and publicized a call for applications for engagements to be executed in the first half of 2020. In 4Q2019, we received 7 applications and selected the following engagements, which will be executed in the first half of 2020 under the new award:

- Franklin & Marshall
- XSEDE Metric Service

---

<sup>38</sup> <https://trustedci.org/application>

- Open Storage Network
- UC Berkeley Secure Research Data and Compute (SRDC) Platform

## 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, an 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 2019 were:

- We had a consultation in 2Q2019 with David McMorries, the new Chief Information Security Officer at Oregon State University, which resulted in his attending a ResearchSOC workshop at EDUCAUSE Security Professionals Conference.
- We consulted with cybersecurity staff from NCAR/UCAR as they were looking for some external guidance for their Cybersecurity governance structure and proposed changes they are considering. We recommended they apply for a late 2020 engagement with Trusted CI.
- We consulted with Jim Beach of the Specify Software<sup>39</sup>, a project with a 30-year history of NSF BIO funding. Jim was looking for guidance on various cybersecurity issues and we pointed him at previous engagements we had done with similar community (LTER, DataONE), our Guide for Cybersecurity Programs, and our Engagement Application process.

## 3.3 REED+

The Research Ecosystem for Encumbered Data (REED+) project at Purdue University (<https://www.rcac.purdue.edu/compute/reed>), funded under the Office of Advanced Cyberinfrastructure (OAC #1840043<sup>40</sup>), has the vision to implement a cost-effective ecosystem to manage regulated data. Driven by need to protect Controlled Unclassified Information (CUI) in research sectors, e.g., defense and aerospace, REED+ intends to address the compliance requirements by using a framework.

The foundation of REED+’s framework will integrate NIST SP 800-171<sup>41</sup> and other related publications, including NIST’s Cybersecurity Framework (CSF)<sup>42</sup> and the Big Ten Academic Alliance<sup>43</sup>. This framework will serve as a standard for campus IT to align with security regulations and best practices. Leveraging the framework, REED+’s vision is then to create a single process for intake and contracting, and to facilitate easy mapping of controlled research

<sup>39</sup> <https://www.sustain.specifysoftware.org/>

<sup>40</sup> [https://www.nsf.gov/awardsearch/showAward?AWD\\_ID=1840043](https://www.nsf.gov/awardsearch/showAward?AWD_ID=1840043)

<sup>41</sup> <https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final>

<sup>42</sup> <https://www.nist.gov/cyberframework>

<sup>43</sup> <http://www.btaa.org/>

to cyberinfrastructure (CI) resources for the Sponsored Programs Office (SPS), Human Research Protection Program, which oversees the IRB, and Export Controls and Research Information Assurance (ECRIA) and Information Technology at Purdue (ITaP) Research Computing division (formally the Rosen Center for Advanced Computing, or RCAC). The overarching goal of this framework is to enable researchers, administrators, and campus IT to better understand previously complicated data security regulations affecting research projects.

We engaged with the REED+ team at Purdue during 1-2Q2019 to assist in developing the framework. The initial steps in the engagement were a review of existing documents and processes, followed by exploring proposed policies. We found the flow of REED+ framework sound, and soon switched to working with Preston's team in focusing on specific aspects of the process, e.g., providing controlled research 'use cases'. The engagement proved especially rewarding, as both the REED+ researchers and Trusted CI came away from the engagement with a greater understanding in the nascent and vanguard processes involved in handling CUI compliance in the domain of research and education.

Additionally, during the engagement, Preston Smith presented on the REED+ framework through Trusted CI's webinars (see Section 1.3).

### 3.4 American Museum of Natural History

The American Museum of Natural History<sup>44</sup> (AMNH) conducts research and education activities spanning multiple branches of science. Scientific collaborations require high network capacity among scientific instruments, collaborators, and researchers. The National Science Foundation (NSF) awarded AMNH funds (OAC award #1827153) to develop and install a Science DMZ to enable high speed transfer of large datasets. Connections were deployed regionally via NYSERnet and nationally via Internet2. Additionally, AMNH's ADFS identity management system was federated with InCommon to give researchers access to Globus data transfer nodes (DTNs).

Trusted CI's engagement with AMNH initially focused on developing an information security program tailored to the new Science DMZ. This effort began by reviewing existing AMNH policies and procedures which might apply to the Science DMZ. After this initial examination, it was decided that the accelerated timeline for installation and configuration of both the Science DMZ and the ADFS federation with InCommon left little time for refinement of a few security policy documents. Instead, effort was focused on fine-tuning system configuration for the Science DMZ by consulting outside expertise from ESnet.

Trusted CI documented the activities of this engagement in a final report<sup>45</sup>. AMNH intends to document the processes of installation and configuration of their Science DMZ and the

---

<sup>44</sup> <https://www.amnh.org>

<sup>45</sup> <http://hdl.handle.net/2142/105406>

federation of their ADFS identity management system with InCommon. This documentation may give other similarly sized institutions a good starting point for installation of a Science DMZ or ADFS integration with InCommon.

The Trusted CI-American Museum of Natural History engagement began January 2019 and finished June 2019.

### 3.5 Polar Geospatial Center

Trusted CI began an engagement with the Polar Geospatial Center (PGC) in January 2019. PGC is a University of Minnesota center providing geospatial support, mapping, and GIS/remote sensing solutions to researchers and logistics groups in the polar science community. PGC is a steward of high volume GIS data which is used to provide a variety of services to the polar research and logistics community. PGC's primary funding sources include NSF Division of Advanced Cyberinfrastructure (ACI) (award 1614673), NSF Office of Polar Programs (OPP) (award 1559691), and NASA HQ (grant NNX16AK90G).

We used the Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects and the related templates<sup>46</sup> to assist PGC in developing their cybersecurity program. We identified and documented PGC's key assets and defined asset-specific controls, policies, roles, and responsibilities in regards to protecting them. In April, we helped PGC to perform a risk assessment of their key assets using the Trusted CI Risk Assessment Matrix. The results for this were used to prioritize security efforts and can be used in the future to inform PGC's ongoing cybersecurity efforts. We consider this engagement to be a major success, largely due to the very active role the PGC team took in the engagement activities.

In the early stages of this engagement PGC leadership expressed concerns regarding any mention of security efforts in regard to the data set and sources PGC relies upon to perform their responsibilities. We were ultimately unable to mitigate these concerns through discussion and revisions of the content and chose not to post an announcement of the engagement to the Trusted CI blog<sup>47</sup>. At the end of the engagement, PGC drafted the content of a closing blog post to briefly describe the activities carried out during the engagement period. As described in our blog post<sup>48</sup>, in early July we delivered a report to PGC describing engagement activities and providing recommendations for future cybersecurity efforts.

---

<sup>46</sup> <https://trustedci.org/guide>

<sup>47</sup> <https://blog.trustedci.org/>

<sup>48</sup> <https://blog.trustedci.org/2019/07/trusted-ci-completes-engagement-with.html>

## 3.6 Scripps Institution of Oceanography

**Background.** Trusted CI began an engagement with Scripps Institution of Oceanography (SIO)<sup>49</sup> in January 2019. SIO is part of the University of California San Diego (UC San Diego) and is supported by multiple NSF awards, including # 1327683<sup>50</sup>, 1212770<sup>51</sup>, and 1556466<sup>52</sup>, as well as research awards from the Department of Defense and National Oceanographic and Atmospheric Administration (among others).

This engagement was a collaboration between Trusted CI and the DOD-funded Principles-Based Assessment for Cybersecurity Toolkit (PACT) project,<sup>53</sup> with Trusted CI providing specific expertise on academic and research environment cybersecurity. PACT is a methodology and tool set based on the Information Security Practice Principles and developed in collaboration by Trusted CI, the IU Center for Applied Cybersecurity Research<sup>54</sup>, and Naval Surface Warfare Center Crane. Lessons learned from applying the methodology to SIO will be used to refine PACT.

Our engagement focused on evaluating SIO's current cybersecurity efforts at a programmatic mission level; diving deeper into implementation details at the Coastal Observing Research and Development Center (CORDC); and making specific, prioritized recommendations for improvement. To assist us in understanding the current state, we used a variety of methods for gathering information throughout the engagement process. These included a weekly drumbeat meeting with SIO engagees, two site visits that included in-depth interviews with a wide variety of SIO and UC San Diego staff, and teleconferences with senior UC San Diego leadership. We also corresponded with engagees through written requests for information and follow-up discussions based on the answers provided, starting first with the 71 baseline questions provided by the PACT process, and then branching into other areas. We delivered the final report in October.

Our engagement with the Academic Research Fleet was a direct result of relationships formed during this engagement.

---

<sup>49</sup> <https://scripps.ucsd.edu/>

<sup>50</sup> [https://www.nsf.gov/awardsearch/showAward?AWD\\_ID=1327683&HistoricalAwards=false](https://www.nsf.gov/awardsearch/showAward?AWD_ID=1327683&HistoricalAwards=false)

<sup>51</sup> [https://www.nsf.gov/awardsearch/showAward?AWD\\_ID=1212770](https://www.nsf.gov/awardsearch/showAward?AWD_ID=1212770)

<sup>52</sup> [https://www.nsf.gov/awardsearch/showAward?AWD\\_ID=1556466](https://www.nsf.gov/awardsearch/showAward?AWD_ID=1556466)

<sup>53</sup>

<https://itnews.iu.edu/articles/2018/IU%20Center%20for%20Applied%20Cybersecurity%20Research,%20NSWC%20Crane%20join%20forces%20again%20.php>

<sup>54</sup> <https://cacr.iu.edu/principles/>

## 3.7 Singularity

During the first half of 2019, we applied the First Principles Vulnerability Assessment (FPVA) methodology to look for vulnerabilities affecting the high value assets in the Singularity container system. We assessed Singularity version 3.1, using containers bootstrapped from the Singularity Library using the Ubuntu:18.04 image. Given the time constraints, the assessment was limited to the shell, exec, and run commands. In Q2, we focused on the Component Analysis step, inspecting the parts of the code related to privileged operation and system access. As a result we found a bug and a configuration issue.

The bug was that containers running in the background cannot be killed by the calling user without creating a new shell. If a malicious container is submitted using a local resource management system and executed on a remote machine, then it will run until killed by the system administrator.

The configuration issue was an unusual ownership of the password file inside of a container and of the root directory. The password file on Linux is typically owned by root, not a regular user. In the current implementation, a regular user can add new entries to this file, creating a system account with a known password. The same is true for the root directory. We note that that is not the case in the assessed system. While we have no current exploits for this case, it is worth tracking by the Singularity team.

The final report<sup>55</sup>, which will be released on January 15, 2020, included, in addition to the above mentioned issues, a discussion of the parts of Singularity that were inspected but where no apparent issues were found. We also commented on design complexities that appear fragile and need special care to prevent future vulnerabilities from being created when the software is updated.

## 3.8 Globus

During the second half of 2019, we started applying the First Principles Vulnerability Assessment (FPVA) methodology to look for vulnerabilities affecting the high value assets in Globus Auth. There are no public version numbers of Globus Auth. The software we are assessing was published in 2019-08-23, and was running in production from 2019-08-21 until 2019-09-11. The git tag was named “release/production/2019-08-21.0”. This software was given to the Trusted CI team packed in Docker containers which differs from the real production environment which is the Amazon cloud. We finished FPVA steps 1, 2, and 3, which are about understanding the architecture, resources, and privilege of the software being assessed, and are currently performing step 4, which is the component analysis.

---

<sup>55</sup> <http://hdl.handle.net/2142/104612>

This engagement is experiencing a two month delay due to a serious illness of one of the persons involved in this assessment. We had to find a different student for this task, and despite finding a very good student, as expected, it took him some time to catch up with the software to assess and the methodology we use.

### 3.9 SLATE

In the second half of 2019, Trusted CI and the Services Layer at the Edge (SLATE) projects collaborated on developing a cybersecurity plan for the SLATE system.

SLATE<sup>56</sup> is funded by an NSF grant managed by the Office of Advanced Cyberinfrastructure (Award #1724821). SLATE accelerates collaborative scientific computing through a secure container orchestration framework focused on the Science DMZ, enabling creation of advanced multi-institution platforms and novel science gateways. The ATLAS collaboration at the CERN Large Hadron Collider has an R&D program utilizing SLATE to centrally operate a distributed data delivery network having service endpoints at multiple computing facilities in the U.S., CERN, the UK, the Czech Republic and Germany, and has evaluated a cache deployed using SLATE within the ESnet backbone in Sunnyvale, California. Similar approaches are already in production (the Open Science Grid data federation which is implemented in part using the Pacific Research Platform and Internet2) supporting LIGO and other scientific collaborations but as yet lack a generalized trust framework. While innovation of the new trust model initially is occurring in the context of the OSG and the worldwide LHC computing grid (WLCG), trusted federated edge infrastructures enabling operation of advanced computing platforms will in future be necessary to sustain a wide range of data intensive science disciplines requiring shared, scalable national and international cyberinfrastructure.

The deployment and operation of software through containerized edge services raises issues of trust between many stakeholders with differing perspectives. Resource providers require guarantees that services running within their infrastructure are secure and operated within site policies; platform service developers and operators require flexibility to continuously deliver and compose new cyberinfrastructure supporting their scientific collaborations; edge cluster administrators need visibility and operational awareness while delegating some of their traditional deploy and operate responsibilities to centralized platform teams, following a "NoOps" model<sup>57</sup>; and finally, the application workloads from end-user science communities rely on the foundational capabilities implemented by platform services to realize the full

---

<sup>56</sup> <https://slateci.io/> , [https://www.nsf.gov/awardsearch/showAward?AWD\\_ID=1724821](https://www.nsf.gov/awardsearch/showAward?AWD_ID=1724821)

<sup>57</sup> The meaning of "NoOps" by the SLATE team relates to a federated edge operations model that reduces the effort required by local site administrators operating services as part of a multi-site infrastructure (e.g. a "grid"). Similar terminology has been coined in cloud computing, c.f. <https://searchitoperations.techtarget.com/definition/NoOps>

potential of shared cyberinfrastructure. This engagement broadly focused on developing SLATE’s cybersecurity program in a way that balances these needs.

In the Trusted CI SLATE engagement, we performed an overall security analysis of the SLATE platform, identified trust relationships and key user/administrator workflows, identified a set of needed security policy documents, and began drafting the security policies. We also evaluated container security tools, explored existing applicable OSG and WLCG security policies, and gathered community input on the SLATE security program, resulting in initial consensus around the security policies and procedures needed to enable wider adoption of the SLATE platform.

Community-driven work on the SLATE security program continues through the WLCG SLATE Security Working Group, which is open to all who are interested. Visit <https://trustedci.org/slate> for pointers to current status of the working group and <https://slateci.io/docs/security-and-policies/> for pointers to current SLATE security policies as they are developed.

### 3.10 U.S. Academic Research Fleet

The United States Academic Research Fleet (ARF) is funded by multiple NSF awards consists of eighteen oceanographic research vessels (with two being constructed) organized by University University-National Oceanographic Laboratory System (UNOLS). These ships vary in size and class, from global class vessels to smaller coastal class vessels. These ships are owned by NSF and the US Navy; and also by operating institutions. The ARF supports seagoing research for scientific disciplines that require access to the sea.

Due to the remote nature of the platforms, ARF faces unique cybersecurity challenges. A research vessels relies on complex mix of operational technology and information technology systems for its daily operations. Also the fact that these platforms are operated by different institutions with different policies compounds these issues. This engagement between Trusted CI and ARF worked to evaluate existing cybersecurity practices in use and delivered a unified cybersecurity plan that will serve the security needs of the community and prepare ARF for the International Maritime Organization requirements due to be enforced by 2021.

### 3.11 UNAVCO

We undertook a light-weight engagement with Doug Ertz, Project Manager, from UNAVCO, a non-profit, 501[(c)(3)] university-governed consortium that facilitates geoscience research and education using geodesy (<https://www.unavco.org/>), to gauge their cyberinfrastructure security posture. This was accomplished with the Trusted CI’s Security Program Evaluation survey<sup>58</sup> – a comprehensive questionnaire that not only quantifies a project’s security posture,

---

<sup>58</sup> [https://docs.google.com/document/d/1gEMUZLQ6O-RA0yjlV9MYIF\\_90C3YpUm1LE0ttt9e800/](https://docs.google.com/document/d/1gEMUZLQ6O-RA0yjlV9MYIF_90C3YpUm1LE0ttt9e800/)

but identifies what areas the project needs to focus their resources on for improvement. Doug completed the questionnaire and used the results to enlighten UNAVCO's governance body on the state of their CI security.

## 4 Engagement Evaluations

Since August 2016 we have routinely followed up with prior engagements to assess long-term impact and our own engagement processes. We have received 31 responses to our Engagement Evaluation Questionnaire<sup>59</sup> to date, including 8 responses in 2019. This section begins with a summary of those quantitative responses in the aggregate.

### 4.1 Quantitative Results

We consistently see high ratings of the positive impact of the engagement on the project or facility, and 27 of 31 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 four responses were 4 out of 5 ("Very Likely") on Question 7.

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." The 2019 responses show no clear indication that these barriers are becoming less common among our engagees.

The 23 responses include 19 first time evaluations, 5 first follow-up evaluations, and 2 second follow up evaluations. 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.

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

20 of 31 responses were 5. All 31 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 4 responses indicated any negative impact, each 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.

---

<sup>59</sup> <https://goo.gl/forms/VHL8Gtda2nWMgu9H3>

The most frequently selected responses were:

- Understanding cybersecurity risks to the science mission (20)
- Knowledge / documentation of information assets (20)
- Increased cybersecurity knowledge among staff and personnel (19)
- Improved governance / policy / risk acceptance structure (18)
- Communication of risks to decision-makers and stakeholders (17)
- Selection of better technology or services (14)

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

- 8 responses indicated “Improved governance / policy / risk acceptance structure.”
- 6 responses selected “More security or efficient identity and access management.”
- 5 responses selected “Communication of risks to decision-makers and stakeholders”
- 4 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.

14 responses selected “None.”

13 responses selected “Other priorities diverted attention from cybersecurity.”

8 responses selected “Insufficient staff/budget/resources to make recommended changes.”

6 responses selected “Insufficient project or facility resources applied to engagement.”

**Q6. Which one of the barriers was most significant?**

- 5 responses selected “Other priorities diverted attention from cybersecurity.”
- 4 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)**

27 of 31 respondents selected 5 (“Extremely likely”). 4 respondents selected 4 (“Very 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 7 ratings of 5. 30 of 31 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.** 16 ratings of “much better”; 9 of “somewhat better”; 5 of “about the same”.
- **Quality of communication.** 20 ratings of “much better”; 6 of “somewhat better”; 4 of “about the same”.
- **Quality of deliverables.** 15 ratings of “much better”; 11 of “somewhat better”; 4 of “about the same”.
- **Positive impact on security.** 16 ratings of “much better”; 7 of “somewhat better”; 6 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 31 responses indicated some positive impact broader than the immediately engaged organization (*e.g.*, sibling organizations, campus IT, customers for services offered).

### **Q11. How can Trusted CI increase the positive impact of its engagements?**

20 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 the responses to this question were complimentary of our process and performance.

### **Q12. How can Trusted CI 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 Trusted CI Framework effort and assistance to NSF in drafting the future cybersecurity section of the Major Facilities Guide (fka, Large Facilities Manual). These include more effort at helping NSF projects and facilities prioritize effort.

## **4.2 Qualitative Results**

Here are some examples of qualitative feedback received from prior engagees:

*The engagement was an entirely positive experience for Gemini, and has produced a rich list of recommendations, which in turn generated a manageable list of action items. It is now an internal process to identify the priorities and resources required to implement these changes. The challenge now is to ensure that these "high priority" items are*

*resolved while maintaining a focus on the overall CyberSecurity program goals for this and the coming years.*

*I have said this on multiple occasions, but I am being absolutely sincere when I say that the engagement was an outstandingly professional, humbling, enlightening and enjoyable experience. We are incredibly pleased to have been able to tap into the knowledge and expertise of the amazingly talented group of people that make [Trusted CI] what it is. I will recommend the [Trusted CI] engagement to anybody without a second thought and look forward to further consultations and follow up engagements if at all possible. Thank you kindly for pointing us in the right direction and providing us with the tools that we needed to refocus our efforts.*

*Working with [Trusted CI] was/is a pleasure. The detailed recommendations that came out of the engagement are still successfully being implemented throughout the organization. Having the report, and detailed recommendations allowed the process to survive multiple management and cybersecurity team staff changes. Our security posture, policy framework and overall cybersecurity program have improved considerably as a result of the engagement.*

*There has certainly been no negative impact. Due to our experience with the engagement, we have continued to promote [Trusted CI] throughout our neighbor facilities and have demonstrated the positive effects that have resulted from it (policy management, asset definition, ICS security etc.). The information has been well received. However, there are little available resources to act on implementing recommendations.*

*As always, a huge thank you to the incredible [Trusted CI] team for doing such a fantastic job! It is greatly appreciated!*

*Above all, the whole [Trusted CI] team was amazingly humble and accommodating, so it was a great pleasure working with them.*

*Willingness to take on "out of the box" engagements such as ours. The consultation was extremely helpful, even though we were not the standard client (our engagement occurred much earlier in the software design phase than was usual) that [Trusted CI] expected to work with.*

*The staff were very responsive and proactive in soliciting participation on the cloud security best practices document. Keep up the good work!*

*[Trusted CI] already performs above all of our project's expectations - I do not see how [Trusted CI] can increase positive impact beyond current effort.*

*The [Trusted CI] engagement team were professional, well informed, and willing to go outside of their normal operating expertise to help identify potential solutions to an authentication and identity management system for our project. Their effort is greatly appreciated.*

## 5 Lessons Learned, Challenges, and Project Management

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

### 5.1 Follow-on Funding Award under Award 1920430

In response to NSF 19-514<sup>60</sup>, Trusted CI submitted a proposal to continue serving as NSF's Cybersecurity Center of Excellence for 2020-24. Trusted CI's proposal was funded by NSF under award 1920430<sup>61</sup>. The new award began on October 1, 2019, however funding from 1547272 will carry Trusted CI through to the end of 2019, hence Trusted CI will effectively begin operating under 1920430 as of January 1, 2020. Specifics of this transition are included in Trusted CI's first quarterly report to NSF for the new award.

### 5.2 Basney Named Trusted CI Deputy Director

Jim Basney of NCSA, a founding Trusted CI team member, assumed the role of Trusted CI Deputy Director<sup>62</sup>.

### 5.3 New Subawards: Internet2 and LBNL

In 2019, Trusted CI operated under a supplemental proposal which included increased spending to initiate two new subcontracts:

- Dana Brunson, initially at Oklahoma State and now at Internet2, joined Trusted CI to lead the new Fellows program (see Section 2.9). We initially established a subcontract with Oklahoma State and then transferred it to Internet2, shifting funds for a staff person to support Dana to Indiana University.
- Sean Peisert, at Lawrence Berkeley National Laboratory (LBNL) to advance the OSCRIP (see Section 2.1). This contract took considerable negotiation between IU and LBNL and was not finalized until April.

---

<sup>60</sup> <https://www.nsf.gov/pubs/2019/nsf19514/nsf19514.htm>

<sup>61</sup> [https://www.nsf.gov/awardsearch/showAward?AWD\\_ID=1920430](https://www.nsf.gov/awardsearch/showAward?AWD_ID=1920430)

<sup>62</sup> <https://blog.trustedci.org/2019/03/jim-basney-appointed-as-trusted-ci.html>

## 5.4 Advisory Committee Changes and Meeting

Dr. David Halstead, CIO for the National Radio Astronomy Observatory, resigned from the Advisory committee at the end of the first quarter and was replaced by Eric Cross, Information Technology Manager for the National Solar Observatory (NSO), as another representative from the NSF Large Facility community.

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, has retired. She was replaced on the committee by Michael Zentner, the Director for Sustainable Scientific Software at the San Diego Supercomputing Center, the Director of the HUBzero project, co-PI on the nanoHUB.org project and is succeeding Nancy as Director of SGCI.

Melissa Woo transitioned from Stony Brook University to Michigan State University, with the same title of Senior Vice President for Information Technology (IT) and Chief Information Officer.

The Trusted CI Advisory Committee is:

- Tom Barton, Senior Consultant for Cyber Security and Data Privacy at the University of Chicago.
- Eric Cross is the Information Technology Manager for the National Solar Observatory (NSO).
- 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).
- Michael Zentner, the Director for Sustainable Scientific Software at the San Diego Supercomputing Center, the Director of the HUBzero project, co-PI on the nanoHUB.org project and Director of SGCI.
- Melissa Woo, Senior Vice President for Information Technology (IT) and Chief Information Officer at Michigan State University.

The Trusted CI Advisory Committee was convened on November 19th, proximate to the SC19 conference. All members attended except Mellia Woo, who was in the process of transitioning to her new role at Michigan State. Additional attendees by invitation were: Kevin Thompson of NSF and Ewa Deelman, PI of the CI CoE Pilot project. Feedback from the committee, along with planned Trusted CI actions is:

- Ask engagees to cite both Trusted CI paper and NSF award number.
  - Planned actions:
    - Discuss at next all hands meeting to make all Trusted CI staff aware of the need to make this request.
    - Add reminder to Trusted CI engagement plan template.
- Solicit success stories (quotes) from engagees for use in promotional materials.
  - Planned actions: We need a better process of regularly following up with engagees. We will take on this improvement in 2H2020.
- Look at NIST 800-160 v2.
  - Planned actions: Added the consideration of NIST 800-160 v2 to the Trusted CI Framework 2020 Project Plan.
- In incident report, note that documenting processes is valuable for educating new staff.
  - Planned action: The following text appears in the incident report “Given that these will represent Trusted CI’s first formal policies, Trusted CI will develop procedures to ensure policies are easily locatable and existing and new staff trained in their application.”
- SGCI found a way to send fellows a check rather than having to arrange all their travel. Follow up with Mike about this.
  - Planned action: Von and Mike have conferred. Mike was mistaken and SGCI has been reimbursing travel as Trusted CI. Both agreed to pursue the honorarium approach and keep in touch on this subject.
- Attend a few regional training events to see how the train-the-trainers materials translate.
  - Planned action: Dana plans to attend GPN meeting and will either attend or have someone relevant attend others. We will also encourage future hosts to attend a workshop at another event to gain experience.
- Identify success criteria (impact metrics) for train-the-trainers effort and train the trainers to track the metrics. Establish a feedback process.
  - Planned action: Relevant metrics that are included in project plan:
    - Outcome metric: REN provides training to their membership in 2021.
    - Success metric: Positive statements about training from REN membership.
    - Success metric: Statements about training positive impact from REN members.
- Send the project plan that we submitted alongside the narrative to the AC.
  - Planned action: The Project Plan, Data Management Plan, and References from the proposal have been shared with the advisory committee.

## 5.5 Trusted CI All Hands Meeting

In late March, Trusted CI held our annual face-to-face All Hands Meeting in Chicago. With new team members (Brunson, Hudson, Peisert and their respective staff, plus others), we used the time together to review our ongoing work and seeking out refinements and potential new activities. With the inclusion of additional team members, instead of the previous format of using breakout groups for future development, we tested moving to a lightning-talk style agenda to cover the state of the various activities of Trusted CI. This style has received positive feedback from those new to the group and veteran members as it allowed those new to group to gain a better understanding of Trusted CI's team members and their activities.

## 5.6 Personnel changes

- At IU, five new members joined the Trusted CI team: Ryan Kiser (Analyst), Anurag Shankar (Analyst), Zalak Shah (Analyst), Diana Cimmer (Event Coordinator), and Kelli Shute (Project Manager). Departures were Michelle Bartley, Grayson Harbour, Mary Conley, and Nicholas Wheeler.
- Also at IU, at the end of 2019, Susan Sons will be shifting to an expanded role with the CI CoE Pilot<sup>63</sup>, working closely with Trusted CI PI Von Welch and CI CoE Pilot PI Ewa Deelman to coordinate collaborations between the projects, and with her direct report, Josh Drake, joining Trusted CI as the day-to-day liaison between the projects.
- At UW-Madison, Evan Kivolowitz left the project due to health issues, and was replaced by Ben Kinzer.
- At NCSA, Raghav Sethi joined the project as a graduate research assistant for the Fall 2019 semester. Raghav graduated in December 2019.
- At PSC Andrew Adams and Kathy Benninger took over several of James Marsteller's duties as he accepted a position at Penn State University. Adams assumed Marsteller's position as Chief Information Security Officer and its associated duty as lead of Trusted CI's security program. Benninger took on the roles of PSC Site Lead and LFST Lead.
- Dana Brunson joined the team from Internet2 to lead the Fellows program.
- Sean Peisert and Reinhard Gentz joined the team from Lawrence Berkeley National Laboratory.

---

<sup>63</sup> <https://cicoe-pilot.org/>

## 5.7 ResearchSOC Collaboration

Trusted CI PI Welch also directs the ResearchSOC project<sup>64</sup>, a collaborative security response center under CICI 18-547 (NSF award #1840034). The two projects have distinct roles in the NSF ecosystem:

- Trusted CI is a trusted, technology-neutral cybersecurity leader and consultant.
- ResearchSOC is developing a set of operational cybersecurity services with a sustainability model of for-fee service.

The two projects collaborate in a number of ways:

- The CI Vulnerability program.
- Outreach, e.g. ResearchSOC presented at the NSF Cybersecurity Summit and on Trusted CI Webinars.
- Internal cybersecurity programs and staff - the CISO for Trusted CI (Adams) is the deputy CISO for ResearchSOC, and vice-versa (Krenz).

## 5.8 Sustainability

We are working towards a vision of being fiscally supported through 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<sup>65</sup> (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<sup>66</sup> as well).

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

---

<sup>64</sup> <https://researchsoc.iu.edu/>

<sup>65</sup> <http://cicoe-pilot.org>

<sup>66</sup> See <http://research.cs.wisc.edu/mist/includes/vuln.html>

- 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)<sup>67</sup> (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)<sup>68</sup>: \$2m/2 years is allowing for formalization and broadening the impact of engagement techniques.
- Funding from the Indiana Secretary of State to CACR to help the State of Indiana with computer security response during the 2020 elections<sup>69</sup>.
- Professor Miller and received approximately 0.2 FTE and Dr. Heymann received approximately 0.1 FTE from UW-Madison to teach the software security course based on the materials developed under Trusted CI (see Section 2.5).

## 5.9 Trusted CI Incident Response Report 2019-10-02\_01

Trusted CI inadvertently exposed an embargoed report. This report, from our engagement with Sylabs regarding Singularity (see Section 3.7), was still under discussion when Trusted CI accidentally published it.

To maintain the community's trust and act as a good model, Trusted CI is being as transparent as possible with the community. Through strong communications with Sylabs, Trusted CI ensured there was no harm from the publication, and then, with Sylabs permission, published their internal report on the incident<sup>70</sup>.

To rectify the events that led to the incident, as described in the report Trusted CI will be formalizing internal data sharing and undertaking regular table top exercises to improve its incident response procedures.

---

<sup>67</sup> <https://renci.org/impact/>

<sup>68</sup> <https://cacr.iu.edu/pact/>

<sup>69</sup> <https://indianavoters.in.gov/MVPHome/ElectionSecurity>

<sup>70</sup> <https://blog.trustedci.org/2019/12/IR-2019-10-021.html>

## 6 International Travel and Impact

During 2019, the Trusted CI team undertook the following international travel under Trusted CI funding:

- Von Welch gave the keynote presentation at the International Symposium on Grids and Clouds (ISGC) 2019 & Soundscape Conference in Taipei, Taiwan in April. Von Welch and Jim Basney (traveling under other funding) gave additional presentations at ISGC to highlight Trusted CI work on the Trusted CI Framework and on CILogon. Bob Cowles was also present to extend discussions concerning collaboration with WISE Information Security for collaborating e-infrastructures (WISE)<sup>71</sup>.

## 7 Metrics

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

**Table 3. Trusted CI activity goals and achieved metrics.**

Activity	Measurement Technique	Goals	Achieved
<i>Engagements with NSF projects.</i>	Direct measurement of the number of engagements.	4-6/year depending on complexity.	On track. Seven engagements completed in 2019 (AMNH, Polar Geospatial Center, REED+ Scripps, Slate, ARF, Singularity)
	Post-engagement survey.	High ratings of engagement utility.	On track. See Section 4 for new results.
	Consultations (new)	None.	3 (see Section 3.2)
<i>NSF projects using our best practices, guides, threat model to develop and maintain their own cybersecurity programs.</i>	Reported by NSF projects.	Initially 2-4/year using cybersecurity program guide <sup>72</sup> . Aim to increase linearly.	The NSF Community Cybersecurity Benchmarking Survey performed by Trusted CI identified in 2019 that 6 projects are using the Trusted CI guide.
Cyberinfrastructure Vulnerabilities / <i>Situational Awareness</i>	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 20 Large Facilities Programs represented on our list (65%).

<sup>71</sup> <https://wise-community.org/about-wise/>

<sup>72</sup> In 2019, we plan to modify this goal as we shift to the Trusted CI Framework described in Section 2.6

**Table 3 (continued). Trusted CI activity goals and achieved metrics.**

Activity	Measurement Technique	Goals	Achieved
<p><i>Training</i></p>	<p>Direct measurement of attendance.</p>	<p>50 members of NSF community per year attending.</p>	<p>426 attendees from the NSF community attended training provided by Trusted CI staff.</p> <p>91 people attended the training sessions at the 2019 NSF Cybersecurity Summit.</p> <p>48 attendees at Trusted CI Workshop on Trustworthy Scientific Cyberinfrastructure at PEARC 19</p> <p>15 attendees at Federated Identity Management at SFSCon 2019</p> <p>30 attendees at Log Analysis at SFSCon 2019</p> <p>100 Attendees at Secure Coding Practices and Automated Assessment Tools at SFSCon 2019</p> <p>10 attendees at Cybersecurity TTP BOF at Educause SPC 2019</p> <p>52 attendees at Secure Coding Practices and Automated Assessment Tools at the University of Queensland</p> <p>12 Attendees at Secure Coding Practices and Automated Assessment Tools at Supercomputing 2019</p> <p>8 Attendees at Secure Coding Practices and Automated Assessment Tools at Internet2 Technology Exchange</p> <p>50 Attendees at Secure Coding Practices and Automated Assessment Tools at University of Iowa</p> <p>10 Attendees at Secure Coding Practices and Automated Assessment Tools at Gateways 2019</p>
	<p>Survey of attendees.</p>	<p>100% rating training as valuable.</p>	<p>Of 29 people surveyed for Summit training day, 100% said they would participate in training at future summits. 100% of the responses found the training useful.</p>

**Table 3 (continued). Trusted CI activity goals and achieved metrics.**

Activity	Measurement Technique	Goals	Achieved
<i>Summit</i>	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 57 NSF-funded projects including 12 large facilities.
	CFP response rate.	Increasing CFP response rate each year.	There were 49 responses to the CFPs in 2019, 17 higher than last year.
	Surveys of attendees.	Very strong evaluations on attendee surveys.	A post summit survey received responses from 31 attendees.  To the question “How would you rate your overall experience with the 2018 summit?”, 21 respondents answered that the quality of the summit was Excellent (highest rating), 9 answered Good (2nd highest) and 1 answered Average (3rd highest).
<i>Software Assurance</i>	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 2019, three applicants requested software assessments.
	Number of groups using online training materials	Linear progression each year.	Nothing to report yet.

**Table 3 (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 PEARC '19 , 2019 NSF Large Facilities CI Workshop, Cyberinfrastructure Brown Bag, 2019 Great Plains Network All Hands Meeting, NCSA, ISGC 2019, 3rd NATO NMIOTC Cyber Security Conference, CENIC 2019,2019 Internet2 Global Summit, EDUCAUSE Security Professionals Conference, and the SGCI Bootcamp
	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: 357 Archive views: 1200
	Subscribers to Trusted CI email Lists (new)	Continued growth	Announce: 844 (+144 since 2018) Discuss: 534 (+112 since 2018)
	Large facilities participating in Large Facilities Security Team (new)	Goal is to have all Large Facilities participating.	All 20 Major Facilities and/or their 12 subprograms are participating

## 8 List of All Trusted CI Engagements

**Table 4. 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
American Museum of Natural History	1547272	Review policies, procedures, and configuration details for securing new Science DMZ.
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 4. All Trusted CI Engagements (in progress and completed) under current award (cont)**

Engaged Project	NSF Award # or Category	Engagement Subject
Globus Auth	1835890, 1541450, 1445604	In-depth vulnerability assessment (code review) of Globus Auth.
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
Polar Geospatial Center	1614673, 1559691	Development of a cybersecurity program
REED+	1840043	Protecting CUI
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
Scripps Institute of Oceanography (SIO)	1327683, 1212770, 1556466	Evaluated cybersecurity program based on the PACT
Singularity	1234408, 1547272	In-depth vulnerability assessment (code review) of Singularity.
SLATE	1724821	Supporting development of cybersecurity program.

**Table 4. All Trusted CI Engagements (in progress and completed) under current award (cont)**

Engaged Project	NSF Award # or Category	Engagement Subject
TransPAC	1450904	Supporting development of cybersecurity program.
UNAVCO		
United States Antarctic Program	Operated by National Science Foundation's Office of Polar Programs	Reviewed processes and policies relevant to polar science information security.
United State Academic Research Fleet (ARF)	1823600, 1824571, 1827383, 1827415, 1827444, 1822574, 1822670, 1824508, 1829214, 1830845, 1823566, 1822532, 1823567, 1823042, 1822954, 1827437, 1822905, 1827654, 1834650	Evaluated existing cybersecurity practices in use across fleet and made recommendations for improvement and to help comply with the IMO 2021 requirements.
University of New Hampshire Research Computing Center	1541430	<p>Assistance in developing an information security program.</p> <p>Quick evaluation of information security program with recommendations for improvement.</p> <p>Training for staff.</p>

**Table 5. 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 AARClear activities, disseminate training and other AARC project outputs to US cyberinfrastructure projects, and facilitate EUUS pilot project activities.
HUBzero (2014-15)	Used by multiple NSF projects.	Review of Web Server Security Model and Disaster Recovery Plan documents.
OOI	Large Facility	Assisted in developing cybersecurity program.
LSST	Large Facility	Assisted in developing cybersecurity program.
NEON	Large Facility	Performed cybersecurity risk assessment on the NEON network of sensors and data servers.
CC-NIE (U. Cincinnati & U. Pittsburgh)	1440646 and 1541410	Facilitated peer-to-peer review of cybersecurity programs.
CC-NIE (U. Oklahoma)	1341028	Cybersecurity program review and guidance. Determined engagement was too early and suspended.
NTP	Core Internet infrastructure	Assisted in migration of source code to open source repository, modernization of build and test infrastructure, creating documentation suitable for onboarding new developers, and pruning old code.
DKIST	Large Facility	Assisted in development of a cybersecurity program. Cybersecurity Program Guide was key output.
Globus	Used by many NSF projects.	Conducted cybersecurity review of the architecture and design of the new sharing functionality.

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

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