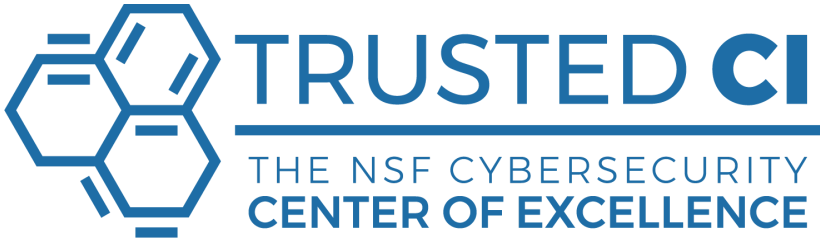


Annual Report for Project Year 1

Trusted CI
The NSF Cybersecurity Center of Excellence

NSF Grant ACI-1920430

October 1, 2019 - September 30, 2020

For Public Distribution

Trusted CI Team

Ishan Abhinit[2], Andrew Adams[1], Emily Adams[2], Kay Avila[3], Jim Basney[3] (co-PI), Kathy Benninger[1], Leslee Bohland[2], Dana Brunson[5] (co-PI), Diana Cimmer[2], Robert Cowles[7], Adrian Crenshaw[2], Jeannette Dopheide[3], Josh Drake[2], Shane Filus[1], Terry Fleury[3], Reinhard Gentz[6], Grayson Harbour[2], Elisa Heymann[4], Florence Hudson[7], Craig Jackson[2], Benjamin Kinzer[4], Ryan Kiser[2], Mark Krenz[2], Jason Lee[6], Barton Miller[4] (co-PI), Sean Peisert[6], Ranson Ricks[2], Ian Ruh[4], Scott Russell[2], Anurag Shankar[2], Kelli Shute[2], Jinyue Song[6], Susan Sons[2], Von Welch[2] (PI), John Zage[3]

[1] Carnegie Mellon University/PSC

[2] Indiana University/CACR

[3] University of Illinois/NCSA

[4] University of Wisconsin-Madison

[5] Internet2

[6] Lawrence Berkeley National Lab

[7] 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 1 (PY1) of Trusted CI under NSF grant 1920430, which took place from October 1, 2019 through September 30, 2020. For the period from October 1, 2019 - December 31, 2019 the majority of project activity took place under the prior NSF award 1547272. For details on those accomplishments, please refer to the 2019 annual report for award 1547272.[1]

Prior to grant 1920430, Trusted CI was supported under NSF grants 1547272 and 1234408.

Please cite this report as:

> Trusted CI Annual Report for Project Year 1. September 2020.
> http://hdl.handle.net/2022/25800

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

[1] http://hdl.handle.net/2022/24873

Trusted CI Project Year 1 Highlights

A. Trusted CI undertook a series of actions to support the community during the COVID-19 pandemic, including:

    a. Issuing a coordinated call [in conjunction with the Science Community Gateway Initiative (SGCI) and CI CoE pilot] for priority support to science projects working on tackling the COVID-19 pandemic.
    b. Producing blog posts relevant to working at home and the increased use of Zoom caused by the pandemic.
    c. Hosting a virtual Town Hall to discuss the impact of the pandemic on the NSF community.

B. We began a series of new project activities, including the annual challenge, office hours, and a collaboration with the QUILT as detailed in the project execution plan.

C. We received confirmation from a prior engagee, the Academic Research Fleet, that they were able to secure additional funding as a result of our engagement report delivered in 2019.

D. The Trusted CI webinar series hosted nine talks with 245 total attendees across 51 NSF projects, and over 461 views. Trusted CI has now impacted over 400 NSF projects through its webinars, engagements, and other activities.

E. We completed 3 engagements in the first half of 2020. We received 7 applications for engagements occuring in the 2nd half of the calendar year and accepted and initiated engagement with 4 of those applicants. We opened the application period for engagements occurring in the 1st half of 2021 and have already received one application.

F. Trusted CI made the decision to remove language with racial biases from new and existing materials.[2]

G. As a result of the pandemic, the program committee and project leadership elected to hold the 2020 NSF Summit virtually this year for the first time in its history. The program and organizing committees leveraged a virtual conference platform to maximize the benefit to the community.

H. The Trusted CI team partnering with the Science Gateways Community Institute (SGCI) worked directly with 6 science gateways during the year and delivered a cybersecurity presentation at SGCI's Jumpstart week.

[2] https://blog.trustedci.org/2020/06/removing-biased-language.html

I. In collaboration with the CI CoE pilot, the Trusted CI team conducted an engagement with the US Academic Research Fleet focused on improving the state of identity management. We also began planning for two additional engagements, one with GAGE and another with SCiMMA. The identity management collaboration team contributed to the pilot's document intended to lay the foundation for a future CI center of excellence.

J. The transition to practice (TTP) cohort onboarded its second member, Shantanu Chakrabartty, from Washington University. In addition, we added two success stories highlighting successful transitions to practice by both Patrick Traynor (University of Florida) and Jay Yang (Rochester Institute of Technology).

K. We welcomed 3 new members to the Advisory Committee: Ewa Deelman, Anita Nikolich, and Damian Clarke. Tom Barton and Nicholas Multari stepped off with our sincere thanks.

L. Kelli Shute accepted the role of Trusted CI Executive Director to ensure our broad team of experts continues to move forward in an effective and coordinated manner.

M. The Cyberinfrastructure Vulnerabilities service alerted the community to 15 critical vulnerabilities after evaluating a total of thirty-four.

Table of Contents

1 Building Community

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

1.1 NSF Cybersecurity Summit

Background. In 2020, we organized the NSF Cybersecurity Summit, which we have been hosting since 2013. The Summit brought together leaders in NSF cyberinfrastructure and cybersecurity to continue building a trusting, collaborative community addressing the community's core cybersecurity challenges. The first day of the Summit was dedicated to training sessions. The second and third days were for the plenary presentations. This year's event took place virtually (due to the pandemic) from September 22nd to the 24th.

Progress this year. We convened the program committee, consisting of volunteers from higher education and NSF large facilities. Jim Marsteller of Penn State University served as the program committee chair. The program and organizing committees elected to host a virtual summit this year to continue to serve the community in a safe way.

The organizing committee evaluated many virtual event platforms and selected Whova[3] for this year's event. IU conferencing provided logistical support for the Summit. This year had our highest registration numbers, with totals over 400.

The first day consisted of 5 half-day training workshops in the afternoon. Training sessions were:

- Tackling Cybersecurity Regulations: DARS, CMMC, HIPAA, FISMA, and GDPR (Anurag Shankar, Erick Deumens, Gabriella Perez, Scott Russell)
- Security Log Analysis (Mark Krenz, Ishan Abhinit)
- Developing Cybersecurity Programs to Support NSF Science (Craig Jackson, Bob Cowles)
- Leveraging AI/ML for SOC Threat Hunting and Incident Investigation (Jay Yang, Ryan Kiser, Emily Adams, Scott Orr)
- Web Security and Automated Assessment Tools—Theory & Practice (Bart Miller, Elisa Heymann)

We also offered 3 pre-recorded training sessions and 3 pre-recorded plenary talks which will remain viewable until March 15, 2021.

[3] https://whova.com/

- Trainings
    - Both Sides of the Looking Glass: How Vulnerability Scanning and Honeypots Can Work Together in Proactive Cybersecurity Operations (Richard Biever, Ken Goodwin)
    - Using a Digital Forensics Tool to Analyze ENRON data (Ebru Cankaya)
    - Foundations of Secure CI (Ciprian Popoviciu, Samir Tout, Lola Killey)
- Plenaries
    - Protecting the Routing Cyberinfrastructure through Machine Learning and Statistical Analysis (Pablo Moriano)
    - Cybersecurity is a Team Sport (Susan Frank)
    - Client Tools for Transitioning from X.509 to Oauth2 Access Credentials (Dave Dykstra)

Days 2 and 3 were each a half day to minimize Zoom fatigue. The Summit keynote speaker was Kate Starbird, who was invited by the program committee, and spoke on “Disinformation”.

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 applied to the program by writing a brief essay sharing their security interests and what they hoped to gain from the Summit. This year, the committee received 60 applications. While we traditionally accept 5 students in the program, we accepted more than 30 students to the program this year.

Plans for next year. Discussion of location and date will be determined at a later date. Due to uncertainty of COVID-19 we will need to reevaluate in January/February 2021 if we will hold the event in-person or shift to a virtual event again.

1.2 Large Facility (LF) Outreach

Background. In January 2017, we convened a working group for information security staff at NSF Large Facilities (LFs), which aims to develop a working relationship between those responsible for cybersecurity across the LFs and to advance the development and implementation of best practices, standards and requirements within the community. This working group, the Large Facilities Security Team (LFST)[4], includes membership from all 20 LFs and uses a combination of a dedicated mailing list and monthly conference calls hosted by Trusted CI to communicate and coordinate effort.

Progress this year. LFST’s ongoing monthly community conference call series continued with topics covering effective cybersecurity policy implementation, the Cybersecurity Assessment Parameter Profile, and a discussion of cybersecurity issues related to sites’ COVID-19 responses. Trusted CI’s LFST leadership team established regularly scheduled monthly calls to coordinate

[4] https://trustedci.org/lfst

group management. Multiple LFST members responded to an outreach effort requesting their suggestions regarding potential call topics and leads.

LFST's monthly conference call series continued in the second quarter with a set of calls focused on documentation of information assets, classifying information assets, and the use of additional and alternate controls (beyond those in a typical baseline security control set). These discussions served as both an opportunity for information sharing among the LFST members and as input to development of the Trusted CI Cybersecurity Framework. Planning for calls in the next quarter was started.

A presentation by NSF's ResearchSOC was featured in the first LFST community call of the third quarter. ResearchSOC team members presented LFST with an overview of ResearchSOC capabilities, ResearchSOC's relationship with Trusted CI, and an update of initial lessons learned from the onboarding of NRAO (an actively participating LFST member). The call included Q&A, with LFST members particularly interested in learning more about the security services that are available through the ResearchSOC. The August call was a facilitated discussion among the LFST member sites of risk, primarily regarding risk acceptance (how it should work and how it does work at the LFST sites), and also extending to risk mitigation and escalation. The September call was cancelled as it overlaps with Trusted CI's Cybersecurity Summit. Planning is underway for calls to resume in the fourth quarter.

Metrics. The following tables summarize LFST metrics and activities for each quarter of 2020.

Table 1. LFST metrics and activity summary - 1Q2020.

Metric	**Status**
Monthly Calls scheduled and participation	Calls were held in Jan, Feb, and Mar. Average attendance is eight (non-Trusted CI) LFST members.
LFST site representation	All LFs are represented directly or through their subprogram(s)
LFO Engagement	Email to LFO introducing Trusted CI's new LFST project lead
Trusted CI and related events publicized to LFST	● CI CoE IdM WG announcements ● ResearchSOC Webinars ● COVID-19 and Zoom advisories ● Trusted CI Engagement application

Table 2. LFST metrics and activity summary - 2Q2020.

Metric	**Status**
Monthly Call scheduled and participation	Calls were held in Apr, May, and Jun. Average attendance was eight (non-Trusted CI) LFST members.
LFST site representation	All LFs are represented directly or through their subprogram(s)
LFO Engagement	Correspondence with NSF updates for Trusted CI links on NSF web pages and LFO workshop status.
Trusted CI and related events and announcements publicized to LFST	● Trusted CI Webinars ● CI CoE IdM WG announcements ● ResearchSOC / CI CoE Workshop ● ResearchSOC Webinars ● Vulnerability announcements

Table 3. LFST metrics and activity summary - 3Q2020.

Metric	**Status**
Monthly Call scheduled and participation	Calls were held in Jul and Aug with 6 and 12 (non-Trusted CI) LFST members attending respectively.
LFST site representation	Confirming and updating LF site representatives.
LFO Engagement	Quarterly contact with LFO for updates and a question about site representation on LFST.
Trusted CI and related events and announcements publicized to LFST	● Trusted CI Webinars ● Trusted CI Office Hours announcements ● CI CoE IdM WG announcements ● ResearchSOC / CI CoE Workshop ● ResearchSOC Webinars ● Vulnerability announcements ● Security-related ESnet Lunch & Learn talk

Plans for next year. We plan to continue fostering LFST representation and member participation in the monthly community calls, sharing Trusted CI and other security-related

announcements and training opportunities with the group, and maintaining contact with NSF's LFO.

1.3 Webinar Series

Background. The Trusted CI webinar series[5] began in 2016 and has become a popular outreach channel for promoting the work of the NSF security community and for sharing information about Trusted CI projects and events. The webinar series aligns with Trusted CI's mission to develop a cybersecurity ecosystem that enables trustworthy science. Presenters are chosen through a combination of an open call for participation and invitations by Trusted CI staff.

Metrics. Table 4 shows the number of webinar attendees and archive viewers in 2020.

Table 4. Trusted CI Webinar attendance and archive viewing.

Month	Topic	Speaker(s)	Attended[6]	Watched Later[7]
Jan.	REN-ISAC	Kim Milford	14	55
Feb.	FABRIC	Anita Nikolich	32	114
Mar.	OnTimeURB	Prasad Calyam	20	40
Apr.	Secure Data Architecture	Arjan Durresi	20	92
May	Software Security	Barton Miller & Elisa Heymann	34	38
Jun.	ResearchSOC	Susan Sons	28	40
Jul.	EPOC[8]	Doug Southworth	34	31
Aug.	TTP Success Stories	Hudson, Kiser, Traynor, & Yang	63	75
Sep.	ACCORD-COVID	Hutchins & Nguyen	n/a	n/a
Total			**245**	**485**

- Webinar registrants added to Announcements mailing list in Y1: 87
- Webinar registrants added to the Discuss mailing list in Y1: 80

Plans for next year. Reach out to potential presenters in Y2Q1 by building a mailing list of NSF awardees and booking presentations. In Y1 we held back a few reservations in order to send invitations focused specifically on this year's Annual Challenge of Trustworthy Data. We will do the same next year once we have selected the topic.

[5] trustedci.org/webinars
[6] Does not include Trusted CI staff and presenters.
[7] Viewed later on YouTube, as of September 9, 2020.
[8] Engagement Performance Operations Center

1.4 Science Gateways Community Institute Partnership

Background. Trusted CI and the Science Gateways Community Institute[9] partner to co-fund half of a cybersecurity analyst to help make science gateways more secure and trusted. Trusted CI is part of the incubator solution area[10] within SGCI and works closely with that team (led by Claire Stirm at SDSC) to provide cybersecurity education and training for the gateways community.

Progress this year. The cybersecurity team has worked with 6 science gateways during 2020. COSMIC2 (NSF Award# 1759826), Hydroshare (NSF Award# 1664061), ChemCompute, COIN-OR, Data@Risk, and Galaxy (NSF Awards #1840003, 1931531, and 1929694). We also gave a cybersecurity presentation at the SGCI Jumpstart! online conference and provided the SGCI project itself with security recommendations.

We continued the engagement with COSMIC2 from 2019, finishing in March with a final report providing recommendations for reducing cybersecurity risk. We also helped COSMIC2 through a security incident, extending the engagement by 2 weeks and providing them with experience with a real incident. On Hydroshare, the team reviewed their Django setup. During the review of Hydroshare's iRODS and Jupyter setup, their team decided to postpone the engagement due to lack of resources.

On ChemCompute, the team has provided the project lead with information on how to start a security program by starting an asset inventory, an Acceptable Use Policy and a Master Information Security Policies and Procedures document. Trusted CI also evaluated and made recommendations on securing their integration with JupyterHub.

We had initial consultations with COIN-OR, but they have decided to postpone their engagement til later in 2020 due to time constraints on their end. We held an initial meeting with Data@Risk and asked them to provide our team with a basic architecture diagram of their planned system. We are awaiting this.

Starting in July, Trusted CI began its engagement with Galaxy. As part of the partnership with SGCI, it was agreed that some of the time allocated to working with SGCI would be allocated to the Galaxy engagement since Galaxy is a science gateway. More information can be found about the progress of this engagement in the Galaxy section of this report.

SGCI moved their June Focus Week to an online format called Jumpstart!, which featured a selection of sessions from their normal Focus Week. The cybersecurity session provided by Trusted CI was attended by close to 40 participants and received good audience participation and questions throughout the presentation. Of the 16 participants that responded to the post

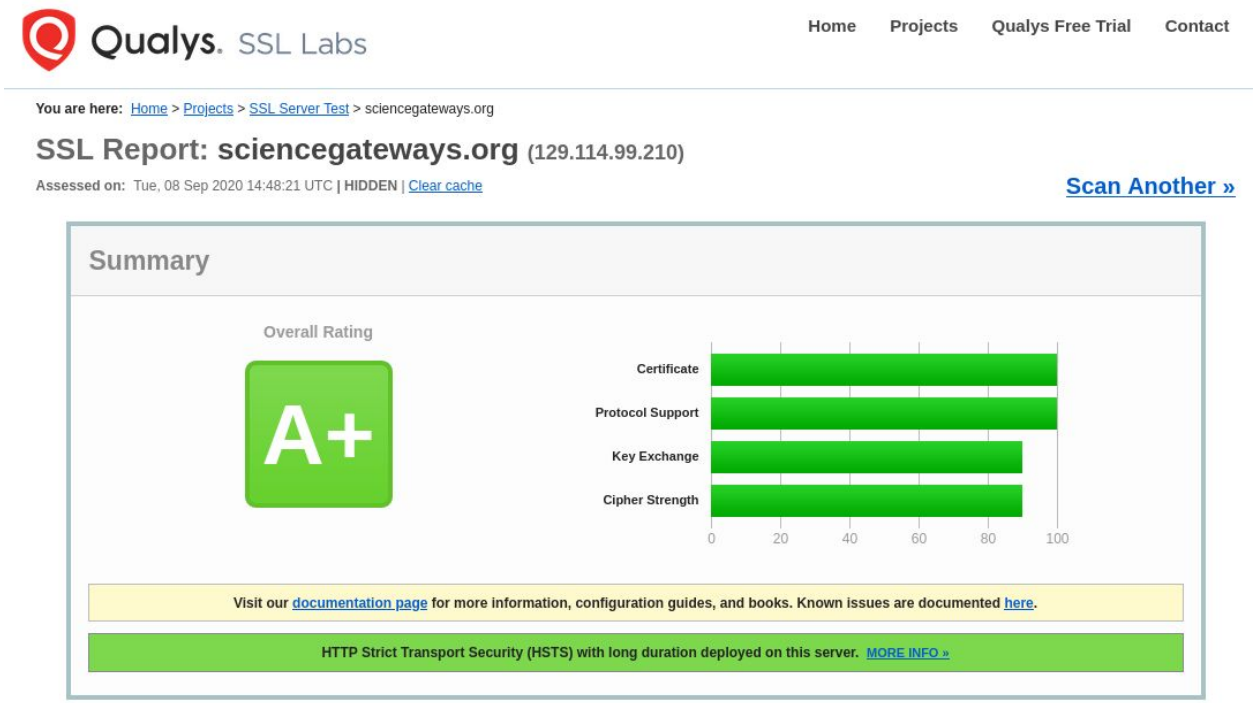
[9] ACI-1547611

[10] https://sciencegateways.org/about/service-areas

session survey, 95% agreed that the speaker was clear in their presentation and 80% stated that they learned something that can help their gateway.

Trusted CI also advised the SGCI team to upgrade their website[11] protocol version to a latest/secure version to avoid any security issues.

Image 1. Output of the ssllabs.com tool showing an A+ rating for the SSL configuration of the sciencegateways.org site.



Plans for next year. We will continue and conclude the engagement with Galaxy, work with gateways projects that request cybersecurity consultation, participate in SGCI's next focus week, and participate in SGCI's upcoming Gateways conference through sponsorship and attendance at the event.

1.5 Trusted CI at PEARC

Background. Second to the NSF Summit, the PEARC conference series is the second highest profile event for Trusted CI. PEARC's impressive attendance (over 800 people) gives members of Trusted CI ample opportunities to network with NSF projects as well as share our work. This year, PEARC20 was held as a virtual conference.

[11] https://www.sciencegateways.org/

Progress this year. The following Trusted CI proposals were accepted for presentation at PEARC20:

- The Fourth Trusted CI Workshop on Trustworthy Scientific Cyberinfrastructure[12], led by Jim Basney
    - This year's workshop included six presentations and hosted almost 70 attendees, a new record for Trusted CI. The presentation topics are listed below:
        - Community Survey Results from the Trustworthy Data Working Group
        - Characterization and Modeling of Error Resilience in HPC Applications
        - Trusted CI Fellows Panel
        - Analysis of attacks targeting remote workers and scientific computing infrastructure during the COVID19 pandemic at NCSA/UIUC
        - Regulated Data Security and Privacy: DFARS/CUI, CMMC, HIPAA, and GDPR
        - Securing Science Gateways with Custos Services
- The Streetwise Guide to Jupyter Security, co-led by Kay Avila.
- Indiana University sponsored a virtual booth at PEARC20. Trusted CI was represented by Todd Stone and as a part of the cybersecurity organizations led by IU.

Not all of our proposals were accepted, however. Despite a strongly favorable review, the software assurance training, by Barton Miller and Elisa Heymann and a compliance workshop, by Anurag Shankar, were both declined. Anurag Shankar's paper, "SecureMyResearch@IU: Baking Security into Research," was declined.

Indiana University was also a sponsor for PEARC, providing additional highlighting of Trusted CI and ResearchSOC.

Plans for next year. We will continue to submit proposals to expand awareness and impact of Trusted CI, including a fifth Trusted CI workshop. 1.6 CI CoE Pilot Collaboration

1.6 CI CoE Pilot Collaboration

Background. Trusted CI and the Cyberinfrastructure CI Center of Excellence Pilot[13] partner to serve the NSF community. Similar to Trusted CI's arrangement with SGCI, the projects co-fund half of a Trusted CI staff member to work with the CI CoE Pilot. Within this partnership, we complete the following activities:

- facilitate identity management working group;
- participate in engagements with NSF large facilities;

[12] https://trustedci.org/pearc20-workshop
[13] https://cicoe-pilot.org/; #1842042

- mature the engagement selection and planning process for the pilot;
- and participate in meetings with the pilot's advisory committee.

Progress this year.

The IdM Working Group was established in January and met monthly throughout the year, hosting discussions and guest presentations of IdM topics relevant to the major facilities. More than twenty representatives from eleven major facilities participated in the working group so far this year. Monthly topics include:

- January: Kick-off meeting
- February: CILogon Presentation by Dr. Jim Basney (CILogon, Trusted CI, NCSA)
- March/May: Roundtable discussion of issues in key-based auth
- April: NEON 2019 IdM Engagement Review: OIDC Connect Implementation with Jeremy Sampson (NEON) and Christine Laney (NEON)
- June: Roundtable discussion on issues in implementing federated identity at NSF major facilities
- July: REFEDS and International Federated Identity with Tom Barton (REFEDS, Trusted CI, UChicago) and Christopher Whalen (NIH/NIAID)
- August: US ARF Engagement lessons learned with John Haverlack (UNOLS, US ARF) and Josh Drake (CI CoE Pilot, CACR)
- September (planned): the Trusted CI framework with Craig Jackson (Trusted CI, CACR) and Ryan Kiser (Trusted CI, CACR)

In May, the IdM collaboration team began an engagement with UNOLS and the Academic Research Fleet to investigate the state of IdM within the fleet's research vessels and shore-side operations. The first milestone, a catalog of current practices in the fleet, was delivered in June. The second milestone, a matrix of IdM tools and services cost and impacts, was delivered in July. The final milestone is on track to be delivered during September: a working proof of concept IdM platform utilizing COManage and OpenLDAP to authenticate ARF endpoints using digital identities federated from users' home institutions. The engagement will run until October.

In July the IdM team began an engagement with GAGE/UNAVCO to assess and design a proof of concept IAM solution. Through the months of July and August the IdM team met with GAGE stakeholders to get an accurate picture of GAGE's IAM needs. The engagement is currently working on the design of a cloud based federated identity proof of concept implementation. The engagement will run until December.

In August, the Pilot jointly hosted a CI/CS workshop[14] with ResearchSOC for major facilities' staff and CI operators. Members of the IdM team helped plan the event, moderated online sessions, hosted office hours, and gave presentations on CI topics to attendees.

The Pilot leadership team drafted vision and blueprint documents to define the vision, mission and strategic objectives of the CoE. A series of interviews was conducted with major facilities to help better understand the needs of the community and findings were integrated into the blueprint. The IdM team is shaping the IdM-related sections of the document.

The IdM team participated in community events and discussions on IAM/IdM topics for the Internet2's IAM Online community and the SciMMA IAM prototype project.

Other Pilot working groups began or continue work on engagements with large facilities:

- ARF-R2R - data lifecycle design
- CHESS - data lifecycle design
- NHERI - participated in SimCenter Workshop and data survey of stakeholders

Plans for next year. The CI CoE Pilot project has received an NCE which should allow us to continue the IdM Working Group through February. We plan to work with them to continue our collaboration through follow-on funding after that date. The IdM team will continue seeking engagements for the purpose of solving and documenting challenges in implementing IAM solutions at NSF major facilities.

1.7 Community Benchmarking Survey

Background. 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.

Progress this year. The 2019 Community Benchmarking Survey was published on Jan 16, 2020. [15] The publication was announced on the Trusted CI Blog and on the Trusted CI announce listserv.[16]

In 2020, the Community Survey project will not be circulating a survey or publishing a report, instead shifting to a 2-year cycle. In Q2 2020, we developed a series of guidance materials to aid future Trusted CI team members when conducting the Community Survey. These materials

[14] https://cics-workshop.org/
[15] https://scholarworks.iu.edu/dspace/handle/2022/24912
[16] https://blog.trustedci.org/2020/01/announcing-2019-nsf-community.html

consist of 1) a "How-To Guide," which walks through a full Community Survey "cycle," and provides an overview of the timeline, key requirements, documents, and roles required; and 2) a baseline series of templates for the key documents, including a templated Community Survey Report, templated Survey question set, and a template for updating the question set.

Metrics. The 2019 Survey Report was viewed 69 times and downloaded 34 times since it's publication.[17]

Plans for next year. During Q4 2020, we will solicit input from the Trusted CI Team on ways to improve the Survey question-set. For CY2021, we will be circulating a full survey, and producing and publishing a corresponding Survey Report by the end of CY2021.

1.8 Presentations

Background. In addition to presentations at other events discussed in this report (in sections 1.1, 1.3 and 1.5), Trusted CI undertakes outreach activities in the form of presentations both to disseminate its work and to make NSF CI projects aware of its services.

Presentations this year.

- Jim Basney, Kelli Shute, and Von Welch presented "Trusted CI: Cybersecurity for Productive, Trustworthy, Reproducible Science" at the National Science Foundation. The slides[18] are available online. [February 2020]
- Von Welch presented "The Mission of Cybersecurity in Science: Productivity, Reproducibility, and Trust" at the SIAM Minisymposium on Transparency, Reproducibility, Sustainability, and Security: The Four Pillars of the Next Generation Scientific Software Stack. The slides[19] and recording[20] are available online. [February 2020]
- Jeannette Dopheide, Anurag Shankar, and Mark Krenz delivered a town hall to discuss the impact of COVID-19 on the NSF open science community. The video[21] and slides[22] are available online for those who were unable to attend. [March 2020]
- Jim Basney and Sean Peisert presented on the BDHubs Data sharing and CI Working Group Call. [March 2020]

[17] As of 9/16/20

[18] https://figshare.com/articles/Trusted_CI_Cybersecurity_for_Productive_Trustworthy_Reproducible_Science/11872137

[19] https://figshare.com/articles/The_Mission_of_Cybersecurity_in_Science_Productivity_Reproducibility_and_Trust/11861781

[20] https://www.youtube.com/watch?index=32&list=PLcntFj46o5pHCub9VeSCCPFJK0xkYq9rs&t=0s&v=t1j3FANzzLc

[21] https://www.youtube.com/watch?v=2s9bp321dJ0&feature=youtu.be

[22] https://www.ideals.illinois.edu/handle/2142/106623

- Scott Russell gave a presentation at the Educause Security Professional Conference on the Department of Defense's Cybersecurity Maturity Model Certification (CMMC)[23] in collaboration with stakeholders from University of Hawaii, University of California San Diego, and University of Washington. The presentation provided a basic overview of CMMC, gave examples of current institutional strategies, and highlighted some key unknowns and challenges CMMC presents. [June 2020]

1.9 Cybersecurity Research Transition to Practice

Background. The purpose of the Trusted CI cybersecurity research transition to practice (TTP) program is to leverage the resources, initiatives, and reach of Trusted CI and their partners such as the OmniSOC and ResearchSOC to enable the deployment of NSF funded cybersecurity research to improve our national and scientific cybersecurity. Deployment could be in NSF large or medium facilities, other NSF projects, research computing, commercial entities, government facilities (agency/lab), or academia. In 2020, based on the success of our Trusted CI Fellows program, we created a TTP cohort program of TTP Fellows to both advance their research and build a community capable of supporting each other in their TTP aspirations and activities.

Progress this year. In 2020, we successfully created a TTP Cohort program (briefly named TTP Fellows), published TTP success stories to inspire researchers to TTP, developed and published a TTP Playbook, including a Technology Readiness Level (TRL) assessment tool and a TTP Canvas, and successfully piloted the first TTP Fellow's cybersecurity research with OmniSOC.

We onboarded the first researcher in the TTP cohort, Jay Yang from Rochester Institute of Technology (RIT), in January 2020. We helped Jay progress the transition of his research to practice in collaboration with OmniSOC and coached him in the development of a clear value proposition for users by leveraging the new TTP Canvas tool developed for the TTP cohort. We onboarded the second researcher to the cohort, Shantanu Chakrabartty and his student Darshit Mehta from Washington University in St. Louis, in March 2020. We have helped Shantanu and Darshit progress the transition of their research to practice through the TRL (Technology Readiness Level) assessment tool and TTP Canvas tool in the TTP Cohort Guide augmented with monthly coaching sessions. We provided Jay and Shantanu the opportunity to present to potential users of their research to identify and nurture TTP opportunities. Shantanu was invited to present his research at the IEEE World Forum for IoT which was cancelled due to COVID-19 and then presented his research in the IEEE/UL P2933 working group special session on clinical Internet of Things (IoT) data and device interoperability with TIPPSS - Trust, Identity, Privacy, Protection, Safety and Security, in May 2020. This resulted in potential TTP connections, for instance a National Institutes of Health (NIH) SBIR/STTR (Small Business

[23] https://events.educause.edu/special-topic-events/security-professionals-conference/2020/agenda/omg-its-cmmc-cybersecurity-maturity-model-certification

Innovation Research / Small Business Technology Transfer) opportunity. Jay Yang presented his research on a Trusted CI TTP Success Webinar in August 2020.

We developed a TTP Cohort Guide including the newly created TTP TRL (Technology Readiness Level) assessment model and TTP Canvas. These tools were developed to help cohort members clarify their goals and plans and enable them to further their TTP efforts. This Guide was developed and piloted with the TTP cohort researchers in 2Q2020. To broaden the impact of the TTP tools we created, we developed a TTP Playbook based on the TTP Cohort Guide and published it on the Trusted CI website[24] including the TRL and Canvas tools. These tools are a key element of the coaching provided to the TTP cohort by Trusted CI and may be used freely by researchers who are not cohort members as well.

The TTP cohort grew further in August 2020 as a result of a TTP Success webinar hosted by Trusted CI on August 11, which attracted 63 attendees, and 68 people who watched the recording afterward. The webinar showcased Patrick Traynor from University of Florida presenting his TTP success story and 2020 TTP Fellow Jay Yang sharing his TTP progress as part of the cohort program. The webinar's inspiring researcher presentations, along with the presentation of the TTP Playbook, TRL and Canvas tools, resulted in four additional TTP researchers joining the cohort. These researchers are from The Ohio State University, Indiana University, University of California at Riverside, and Oak Ridge National Lab (ORNL). The ORNL cybersecurity researcher is a former IU student who presented a poster at the 2019 Trusted CI TTP workshop.

The new TTP success story series[25] launched in January 2020, with the goal to share best practices and learnings from actual research TTP efforts which have succeeded to inspire other researchers to TTP. The goal in 2020 was to publish six success stories, creating an ongoing cadence of TTP success stories. As of July 2020, we have published five as follows with a sixth planned for September, highlighting the research, researcher, and transition path:

- January - Mayank Varia at Boston University with secure multi-party computation for the City of Boston and Boston Women's Workforce Council
- March - Jim Basney at the University of Illinois at Urbana Champaign with CILogon for multiple higher education users
- May - Patrick Traynor at the University of Florida with Skim Reaper for multiple commercial users
- June - Jay Yang at Rochester Institute of Technology with artificial intelligence and machine learning for OmniSOC and Indiana University
- July - Shantanu Chakrabaartty at Washington University - St. Louis with zero-power timer technology for new user opportunities including medical devices

[24] https://www.trustedci.org/technology-transition-to-practice
[25] https://blog.trustedci.org/search/label/TTP

The TTP success stories, TTP playbook, TTP TRL tool and TTP canvas are openly available on the Trusted CI TTP website.[26] We published these to share best practices and tools to inspire and enable researchers to TTP. In September, a draft guide to developing a TTP Canvas will be developed to enable researchers to clarify the use and value of their research, as well as the funding model, activities, and partnerships for TTP success.

Metrics.

- Published five TTP success stories through July with one additional success story planned by the end of the year.
- Onboarded six TTP researchers plus one student to the TTP cohort.
- The first two TTP cohort members completed TRL assessments and TTP canvases based on our templates.
- Published first versions of the TTP TRL assessment tool and TTP canvas tools on the Trusted CI website.

Plans for next year. Lessons learned through work with the Trusted CI TTP Cohort have informed planned changes to the TTP program. Our goals for project year 2 are as follows:

1. Support assessments and experiments to provide needed validation and testing for research to convince users of its value.
2. Support researcher outreach to users and foster productive relationships between researchers and intended users of their technology.
3. Produce communications to motivate and enable NSF funded researchers broadly to transition their research to practice, whether by working with Trusted CI or independently.

In support of goal #1, we will continue to develop and validate the process established in the first half of 2020 to assess research and its utility. These efforts will enable us to provide additional support to cohort members such as identification of user needs, appropriate user communities, and potential partners. These development and validation efforts include further refinements to tools produced in 2020 such as the TRL assessment tool and TTP canvas as well as development of new tools and guidance to aid researchers who are attempting transition research to practice.

In support of both goals #1 and #2, we will work with the cohort members transitioning their research through direct engagement with selected cohort members and identified users to advance the research TRL, develop sustainability plans, advance business maturity according to information identified in the canvas or other activities which serve appropriate TTP goals.

[26] https://trustedci.org/ttp

In support of goal #3 we will continue outreach efforts to communicate with researchers about how they can transition their research to practice both individually and directly with Trusted CI through cohort membership. This will include two additional success stories, a workshop session for researchers to help them to develop a clear and concise value proposition to potential users, and a webinar in the second half of 2021 to describe lessons learned and solicit additional researcher engagement with the cohort.

In addition to these activities, in 2020 we identified refinements to existing processes which we intend to implement in 2021 which will make Trusted CI's TTP efforts more effective. These are as follows:

- We will work to streamline the onboarding process for TTP cohort members. This will allow the TTP cohort to grow more quickly and in an ad-hoc manner as needed with reduced risk of causing bottlenecks due to Trusted CI staff availability.
- Continue development of the TTP TRL assessment tool to more closely align it with and/or map it to other TRL models in use at other organizations.
- Establish additional methods for Trusted CI staff and cohort members to communicate and share information. These will take the form of either a channel in the Trusted CI Slack space, an email list, or both.
- Establish a web presence for the Trusted CI TTP Cohort on the Trusted CI website which describes the cohort, its members, and references any current or future TTP successes of cohort members.

Additionally, a supplemental proposal (request 2053268) on the subject of Transition to Practice was submitted to NSF in 3Q2020. That proposal is pending at the time of this report submission and would add a complementary set of activities with a regional focus.

1.10 Social Media Impact

Background. In order for Trusted CI to be effective, Trusted CI's outreach must reach as much of the NSF community as possible. Social media is part of our strategy for this outreach. This section covers our social media impact, broken down by Twitter impressions[27], blog page views, and unique website visits. Table 3 shows the stats collected in Y1. The last row lists the stats from 2019 and demonstrates a clear growth in our social media impact.

Progress this year. Our social media impact continues to fluctuate with our activities. The sharp uptick of stats in March is likely due to the four blog posts we published as our response to COVID-19 was gearing up. Blog views increased overall in PY1 compared to 2019, likely because we posted more blogs this year compared to last year. We tend to see more activity before and

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

during the Summit. This year it is scheduled for late September and thus not fully represented in this report at the time of publication.

Metrics.

Table 5. Social media impact Y1.

Date	Twitter Impressions	Blog Page Views	Website Visits
Jan.	10.9K	3.9K	1.2K
Feb.	7.1K	2.5K	.9K
Mar.	44.1K	7K	.9K
Apr.	8.2K	4.5K	.8K
May	11.9K	3.9K	1.1K
Jun.	8.3K	1K	1.1K
Jul.	9.4K	5.6K	2.1K
Aug.	8.9K	6K	1.8K
Sep.	No data	No data	No data
Total Y1	**109K**	**34K**	**9.8K**
Total 2019[28] (for comparison)	149.6K	22.6K	11K

Plans for next year. We will continue to utilize Twitter, Blogger, and our website to report our efforts to the public.

1.11 Office Hours

Background. This year, Trusted CI initiated a new activity, monthly "office hours" via online chat (e.g., Slack). Some office hours have topics related to Trusted CI activities (e.g., follow up from a webinar, discussion of a new Trusted CI report, or coordination following a situational awareness alert). Some office hours do not have a preset topic but are an open forum for community members to interact in real-time with available Trusted CI staff. Understanding that many cybersecurity topics cannot be addressed in just one hour, we expect the office hours to generate follow-up activities, such as blog posts, engagements, and webinars.

Progress this year.

We accomplished our goals for Y1, which were the following:

- Review office hours offered by other NSF projects, ask about their experiences
- Write an internal report of lessons learned
- Present a summary of this work to the Trusted CI team
- Assign office hours for the months of July - December (see Table 6)
- Announce the program to our community via a blog post and the discuss list

[28] Since we are calculating January - September 2020, the 2019 tally also represents January - September.

- Kickoff the program on July 23rd
- Continue promoting and monitoring the program
- Assess the successes and lessons learned as the project continues

Table 6. Office hours month, leader and topic.

Month	Leadership POC	Potential Topics/Areas of Expertise
July	Jim Basney	IAM, Trusted CI resources and support
August	Von Welch	1H2021 eng. app. open, Framework, Science Gateways
September	Dana Brunson	2021 Fellows applications
October	Barton Miller	Software assurance
November	Sean Peisert	OSCRP
December	Kathy Benninger	Network Security

Plans for next year. Office hours has had two sessions as of the publishing of this report. We have seen very little activity on the Slack channel thus far, but around a dozen community members have joined the channel. Our impression is that there is some interest in engaging with us but we haven't yet found the right topic or host to draw out those conversations. Our plan next year is to experiment with how to initiate more activity on the Slack channel.

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

Background. The Open Science Cyber Risk Profile (OSCRP) is a community document first developed in 2016 by a working group led by Trusted CI and Berkeley Lab that categorizes scientific assets and their common risks to science to greatly expedite risk management for open science projects and improve their cybersecurity. One of Berkeley Lab's foci is to expand and evolve this document in certain ways. In the first half of 2020, Trusted CI plans to examine the challenges that scientific researchers face when obtaining access to and in using data that is in some way sensitive and subject to restrictions on its access and use in order to protect confidentiality. Trusted CI plans to conduct a survey of the community to understand when and how research is inhibited by current policies and technologies and plans to document the results of this survey for use by the community to help identify paths forward that may better enable scientific progress, and eventually integrate results into the OSCRP. In the later months

of 2020, Trusted CI will augment the OSCRP with results from last year's data integrity white paper and this year's "annual challenge."

Progress this year. Trusted CI developed a survey of questions to ask of the community and reached out extensively in an effort to set up discussions. In particular, we reached out to the executive directors of all Big Data Hubs and presented on the Big Data Hub monthly phone call, among other community-focused efforts. We also spoke with numerous university personnel such as individual scientific contributors, directors of research IT, library staff involved in scientific data curation, and executive university administrators overseeing IT. We have many pages of notes that we have put into a draft report. The first draft of this report was shared with the Trusted CI team and community contributors on 8/7/20. Feedback was incorporated and a second draft shared 8/20/20. Feedback was incorporated and a third draft shared with discuss@trustedci.org on 8/30/20. Responses are requested so that a blog post and a final report can be issued prior to the NSF Cybersecurity Summit. Initial feedback has been *extremely* positive and complimentary as to the value of the document.

Separately, we also began engaging with the authors of the Trusted CI Framework about identifying and building in bi-directional connections between the OSCRP and the Framework to help scientists, research IT, and cybersecurity professionals best understand the key issues and to enable more productive communication with each other.

In conjunction with Jim Basney, who is leading the 2020 Trusted CI Annual Challenge, we submitted a proposal to the NSF 2020 Cybersecurity Summit to jointly present on the 2020 Trustworthy Data Challenge and our 2019 data integrity report findings. Our proposal was accepted and we will be presenting at the summit. In addition, updates to the 2019 data integrity report, based on findings from the 2020 Trustworthy Data Challenge, are being made and will be completed in October 2020.

Finally, we began making draft updates to the OSCRP based on initial findings from the aforementioned integrity survey and also the confidentiality survey currently in progress. A draft of this will be shared with the Trusted CI team in September 2020. Final revisions are planned for November 2020 after suggested changes are incorporated.

Metrics. Trusted CI had 15 highly productive meetings with members of the community that served as input to the data confidentiality report, in addition to a conversation with the monthly "Big Data Hub" phone call. In iterating with contributors to the draft report shared with them, we have received universally enthusiastic and positive feedback on the value of the report.

Plans for next year. We plan to finalize the OSCRP in November. In 2021 we plan to work to tie the OSCRP closer to the Trusted CI Framework by ensuring cross-references between the two

documents and possible re-branding of the OSCRP to something that implies closer ties to Trusted CI and the Framework.

2.2 Situational Awareness / Cyberinfrastructure Vulnerabilities

Background. In collaboration with the ResearchSOC project[29] and community member Scott Sakai of the San Diego Supercomputer Center, Trusted CI manages a situational awareness service that the community can count on for high quality, easy-to-follow notifications on relevant vulnerabilities and threats. Trusted CI tracks notifications from educational and government entities, including, US-CERT, REN-ISAC, NIST, and CISA; news sources, such as The Hacker News, Threatpost, The Register, Naked Security, Slashdot, Krebs, SANS Internet Storm Center, and Schneier; software developers OpenSSL, OpenSSH, and Globus; and leverages our relationships with the NSF Supercomputing Centers (NCSA, PSC, and other XSEDE Service Providers). We filter issues for those relevant to the community and then supply simple guidance to go with those notifications. Trusted CI utilizes its existing email lists and encourages a dialog among those receiving the notifications for further discussions and feedback. All notices are archived and searchable from the Trusted CI email archives.

Progress this year. In 2020, fifteen critical vulnerabilities were communicated to the community after evaluating a total of thirty-four.

Metrics. In 2020, the number of subscribers on the email distribution list increased to 159.

Plans for next year. We intend to operate as expected. Additionally, we intend to instantiate annual surveys to our community in order to better access our impact to the community.

2.3 Publications

Background. Trusted CI team members publish papers on topics valuable to the NSF science community.

Publications this year.

- Reinhard Gentz and Sean Peisert, “An Examination and Survey of Random Bit Flips and Scientific Computing,” December 2019. http://hdl.handle.net/2022/24910
- 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

[29] https://researchsoc.iu.edu/

- Joseph O. Eichenhofer, Elisa R. Heymann, Barton P. Miller and K W. (Arnold) Kang, “An In-Depth Security Assessment of Maritime Container Terminal Software Systems”, IEEE Access, 2020.[30]

2.4 Training

Background. Trusted CI team members deliver training on topics valuable to the NSF science community.

Progress this year. Bart Miller and Elisa Heymann taught a half-day tutorial on Web security and Automated Assessment Tools, at the NSF Cybersecurity Summit. The tutorial included a hands-on segment on web security. September 2020.

Mark Krenz and Ishan Abhinit delivered a half-day training session at the NSF Summit on security log analysis. September 2020.

Craig Jackson and Bob Cowles hosted a training session at the NSF Summit focused on developing cybersecurity programs for NSF science. September 2020.

Bart Miller and Elisa Heymann’s tutorial proposal on Web Programming and Automated Assessment Tools was accepted at Gateways 2020 as a half-day tutorial. The tutorial includes a 1-hour hands-on segment on web security. October 2020.

Plans for next year. Bart Miller and Elisa Heymann’s tutorial proposal on Secure Programming and Automated Assessment Tools was accepted at the Supercomputing 2020 conference as a full-day tutorial. The tutorial includes a 2-hour hands-on segment on web security. November 2020.

Trusted CI will continue submitting proposals to teach tutorials at relevant venues, including Supercomputing, Gateways, NSF Cybersecurity Summit and others.

2.5 Software Assurance

Background. Software is being developed in significant volume by the CI community. Producing software without weaknesses and vulnerabilities is a challenge due to technical barriers and a lack of incentives. Hence, this software can introduce significant risks to the operation of cyberinfrastructure and the science it supports. To address those risks, we work with both software developers and operators to help them measure and manage risks by providing training (on secure coding, secure software engineering, and software vulnerability assessment) and in-depth source code reviews. Software assurance overlaps with Trusted CI's mission to

[30] https://ieeexplore.ieee.org/document/9138421 (DOI: 10.1109/ACCESS.2020.3008395)

lead in the development of an NSF Cybersecurity Ecosystem through training future and current software developers, which directly impacts trustworthy science.

Progress this year. In January, Bart Miller and Elisa Heymann started teaching a 3-credit course, *Introduction to Software Security* (CS639), at the University of Wisconsin-Madison to 80 students (mostly senior Computer Science and Computer Engineering majors). This was an ongoing activity until May 2020. While their teaching time was covered by academic funds, this course was based on the video modules and text chapters prepared under the Trusted CI funding by Miller and Heymann (material available online[31]). The course followed the flipped-classroom model, which means that class time was used for active learning with activities such as group discussions and problem-solving. On March 15, due to the COVID-19 pandemic, instruction changed to be done remotely. They kept their class scheduled and taught remotely using BBCollaborate learning platform. The online version of the class was interactive with live exercises and weekly quizzes.

This course was taught as a "topics" class in 2019 and 2020. It has now been approved as a permanent part of the UW-Madison Computer Sciences curriculum under course number CS542. Having this course as part of the Computer Science curriculum at the University of Wisconsin-Madison allows us to reach future software developers, so that they will produce more secure software. The goal is that we reach as many future developers as possible with these foundational skills.

Miller and Heymann produced a video modules on "Thinking like an analyst: The Manager's Point of View: Responding to a Vulnerability", "FPVA Step 1: Architectural Analysis (part 1)", "FPVA Step 1: Architectural Analysis (part 2)", "FPVA Step 2: Resource Identification", and "How Tools Work", which are available at https://research.cs.wisc.edu/mist/SoftwareSecurityCourse/. All the videos include closed captions for accessibility.

[31] http://research.cs.wisc.edu/mist/SoftwareSecurityCourse/

Image 2. Pictures from Spring 2020 CS639 (Introduction to Software Security) at the University of Wisconsin-Madison

Metrics. For CS639, there were 78 students enrolled as of the last day of class.

Plans for next year. Bart Miller and Elisa Heymann will teach the new approved course CS542 at the University of Wisconsin-Madison in Spring 2021 using the materials developed under Trusted CI.

2.6 The Trusted CI Framework: An Architecture for Cybersecurity Program

Background. The adoption of the Trusted CI Guide to Developing Cybersecurity Programs[32] (the 'Guide') has demonstrated community need for a framework[33] for establishing and maintaining

[32] https://trustedci.org/guide-overview
[33] https://trustedci.org/framework

a cybersecurity program. 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 2020, the Framework is one of our major strategic initiatives. The Framework is both an improvement on and replacement for the Guide, its templates, and related materials. The Guide and its templates have been an important contribution of Trusted CI to the NSF science community and have helped provide structure and material for a number of engagements and training events.

Progress this year. In December 2019, we assembled a team to begin the Framework Implementation Guide development effort. We organized the development into five (5) content groups to be completed throughout the calendar year 2020. In February 2020, we onboarded the Framework Advisory Board (FAB) to assist the team with FIG development through conducting reviews and providing feedback. We established an ongoing monthly series of meetings with the FAB to discuss delivery of new content for review and their input on prior deliverables. We expanded the FAB from 14 members to 19 from NSF major facilities, other NSF projects, ESnet, and institutions of higher education (*see* list FAB members below). Through our collaborative engagement with the FAB, we have made significant progress by completing four content groups that included 11 of the 16 Must chapters. This also included early publication of Must 15 (Organizations must adopt and use a baseline control set). The team began the review and revision of Trusted CI Framework templates that will be referenced in the completed FIG. Finally, we presented training at the 2020 NSF Cybersecurity Summit that focused on Must 15, the CIS Controls, and how to use the Trusted CI CIS Controls v7.1 Tracking Tool.

FAB members and their organizational affiliations:

- Kay Avila (NCSA)
- Steve Barnet (IceCube)
- Tom Barton (University of Chicago)
- Jim Basney (NCSA)
- Jerry Brower (NOIRLab, Gemini Observatory)
- Jose Castilleja (NCAR / UCAR)
- Shafaq Chaudhry (UCF)
- Eric Cross (NSO)
- Carolyn Ellis (Purdue U.)
- Terry Fleury (NCSA)
- Paul Howell (Internet2)
- Tim Hudson (NEON / Battelle / Arctic)
- David Kelsey (UKRI/WISE)
- Tolgay Kizilelma (UC Merced)
- Nick Multari (PNNL)
- Adam Slagell (ESnet)
- Susan Sons (IU CACR)
- Alex Withers (NCSA / XSEDE)
- Melissa Woo (Michigan State U.)

Metrics. The project is on schedule by completing the four content groups planned for this reporting period along with the early release of the Must 15 chapter.

Plans for next year. Complete the remaining Must chapters and front matter, review and update referenced Trusted CI templates, publish the FIG version 1.0, and begin an engagement with Gemini Observatory / NOIRLab as an early adopter.

2.7 Secure Software Engineering Guide

Background. The Secure Software Engineering Guide compliments Trusted CI software assurance efforts by providing a set of touchstone guidelines that NSF research and cyberinfrastructure projects can work from when developing software. This 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".

Progress this year. We completed and published Version 1.0 of the guide[34], 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.

Plans for next year. We'll continue to use the guide as a tool to assist projects trying to adopt secure engineering practices to support the development of software.

2.8 Broader Impacts

Background. Trusted CI is charged with addressing cybersecurity challenges "affecting small projects, multi-institution collaborations, international collaborations and large facilities." There are approximately 500 new NSF projects funded each year at $1 million or more, which we believe is a budget level that indicates that they likely develop/use/operate significant cyberinfrastructure with cybersecurity needs. While we engage directly with NSF projects (via engagements, summits, webinars, mailing lists), we also focus on how to develop and implement strategies which help meet the cybersecurity needs of this broader set of NSF projects (both small and large) and to provide demonstrated value to a significant percentage of NSF projects.

Progress this year. We received notification from Infrastructure Capacity for Biology (ICB)[35] that they leveraged Trusted CI's Framework and templates (including Acceptable Use, Access Management, Risk and Natural disaster policies) to support the creation of appropriate policies for their network.

We leveraged available capacity as a result of the change in the Franklin & Marshall engagement to provide community-wide information and recommendations on current cybersecurity issues, such as how to mitigate the security risks when having to run end of life

[34] https://sweguide.trustedci.org
[35] https://www.nsf.gov/awardsearch/showAward?AWD_ID=1821089&HistoricalAwards=false

software past it's support lifetime. This was brought about due to the recent Windows 7 end of life date on January 1, 2020. This was published as a blog post on the Trusted CI blog[36]. In addition, the team released three other blog posts: one recommends how to deal with a team that must work remotely in response to the COVID-19 crisis, another provides information about security settings within the Zoom video conferencing for requiring a password for by-phone users that were not being covered in other documentation and recommendations, and the last covers the use of password managers.

In July, PI Von Welch was invited by EDUCAUSE to participate with a small group of leaders in higher education to develop a deeper understanding of current initiatives to mitigate security risks to research and to potentially inform potential higher education research community responses to legislative and/or regulatory developments in the future. Additionally, Welch continues to serve on the InCommon Steering Committee as an advisor representing the research community.

One method we use to track the geographical impact of our engagements is to maintain an engagement map for inclusion in presentations. We hadn't updated the map in a while, so this quarter, we refreshed the engagement map (with updates for Google Maps changes) and documented a process for maintaining the map regularly in the future. The current map follows.

Image 3. Engagement map.

[36] https://blog.trustedci.org

We also continued to track project impact on a regular basis. This year, the total number of NSF projects impacted by Trusted CI (over the lifetime of the project) increased to 402 projects from 376, coming from an increase of projects impacted by the monthly webinar as well as the engagements. The total number of NSF projects impacted through the webinar has likewise increased to 141 from 115. We also have begun maintaining a central contact list, and the number of individuals in the directory who have attended a webinar or the summit has increased to 2401 from 1491.

2.9 Fellows Program

Background. On an annual basis, Trusted CI solicits applications from and selects six members of the scientific community (e.g., an IT professional working with a science project) for our Fellows program. We empower them with basic knowledge of cybersecurity and the understanding of Trusted CI's services and then have them serve as cybersecurity liaisons to their respective communities. They then assist members of the community with basic cybersecurity challenges and connect them with Trusted CI for advanced challenges.

Progress this year. Twenty-eight applications were received by January 17 for the 2020 Trusted CI Fellows cohort. These applications were reviewed by members of the Trusted CI leads, 2019 Fellows, and Advisory Committees. The selected 2020 Fellows[37] are:

- Songjie Wang, CI Engineer, University of Missouri
- Tonya Davis, Asst. Professor, Dept of Social Work, Psychology Counseling, Alabama A&M University
- Smriti Bhatt, Asst. Professor of Computer Science, Texas A&M University - San Antonio
- Luanzheng Guo, Ph.D. Candidate, University of California, Merced
- Jerry Perez, Director of Cyberinfrastructure Operations, University of Texas at Dallas
- Laura Christopherson, Senior Data Scientist, Renaissance Computing Institute (RENCI)

The Trusted CI Virtual Institute commenced its weekly sessions on March 25 with sessions as follows:

- Week 1 (3/25): Kick-off meeting, introductions, logistics, overview of Trusted CI.
- Week 2 (4/1): NSF Cyberinfrastructure and the CI Center of Excellence Pilot with Ewa Deelman.
- Week 3 (4/8): Meeting with 2019 Fellows where available, 2019 Fellows share their thoughts and experiences with open discussion.
- Week 4 (4/15): 3 2020 Fellows take 10 minutes each to present their work and discuss goals

[37] https://trustedci.org/current-fellows

- Week 5 (4/22): 3 2020 Fellows take 10 minutes each to present their work and discuss goals
- Week 6 (4/29): “YOU KIDS GET OFF MY LAWN: A CISO confronts Research” with Mike Corn.
- Week 7 (5/6): Components of a cybersecurity program with Craig Jackson
- Week 8 (5/13): Cybersecurity for Research in Europe with David Kelsey
- Week 9 (5/20): Fellows Chat with Dana Brunson to discuss the program, get feedback, and to develop submission to the Trusted CI workshop at PEARC.
- Week 10 (5/27): Identity and Access Management with Jim Basney
- Week 11 (6/2-4): EDUCAUSE SPC virtual - no meeting
- Week 12 (6/10): Cyberattack Anatomy - “Attacker methodology” with Keith Lehigh
- Week 13 (6/17): Fellows Chat with Dana Brunson to discuss the program, get feedback, and explore Fellows participation in Trusted CI Engagements
- Week 14 (6/24): Cybersecurity from a Research Computing Center perspective with Erik Deumens
- Week 15 (7/1): Science DMZ Security with Eli Dart.
- Week 16 (7/8): Security in the Grey Areas with Anita Nikolich.
- Week 17 (7/22): Hacks and Counter-Hacks: How the Bad Guys Think about Your Code and Some Defensive Techniques with Barton Miller and Elisa Heymann.
- Week 18 (7/22): Fellows Chat with Dana Brunson to discuss the program, get feedback and prepare for the Fellows panel at PEARC.
- Week 19 (7/28): PEARC20 - no meeting.
- Week 20 (8/5): Network Security with Kay Avila.
- Week 21 (8/12): UCAR Cybersecurity Program with Jose Castilleja.
- Week 22 (8/29): Cybersecurity and Privacy with Kent Wada.
- Week 23 (9/2): A Day in the Life of a CISO with RuthAnne Bevier.
- Week 24 (9/9): CACR’s Cybersecurity Program with Emily Adams and Zalak Shah.
- Week 25 (9/25): Fellows Chat with Dana Brunson to discuss the program, get feedback and prepare for the Fellows panel at the NSF Summit.
- Week 26 (9/16): ICS/SCADA Cybersecurity with Phil Salkie.
- Week 27 (9/23): NSF Cybersecurity Summit - no meeting.
- Week 28 (9/30): Summit discussion and wrap up.

The sessions with the 2019 Fellows presenting, the current Fellows presenting, and the chat sessions were all new this year as recommended from the 2019 Fellows. Additionally, we are using a form to receive feedback from the Fellows about each speaker, so far with positive feedback. The Fellows presented as a panel to the Trusted CI at PEARC workshop and at the NSF Cybersecurity Summit.

Earlier in the year, the 2019 Fellows reported on some of their outcomes. Aunshul Rege successfully published her work "A social engineering awareness and training workshop for STEM students and practitioners" which was enabled by the Trusted CI Fellows program. Shafaq Chaudhry created a charter for her institution's faculty governance committee to help drive research technology support and provide input on policies and compliance. Jay Yang has begun collaborations with CACR/OmniSOC and the STINGAR project.

Metrics. Twenty-eight applications were received from across the community indicating significant interest in the program.

Virtual Institute Sessions occur weekly except when replaced with EDUCAUSE SPC conference, PEARC and the NSF Cybersecurity Summit. The Virtual Institute included five open chat sessions, 16 sessions with invited speakers plus sessions with previous Fellows and for internal presentations and discussions.

Plans for next year. The call for 2021 Trusted CI Fellows will open at the NSF Cybersecurity Summit and be due later this fall. The 2021 Trusted CI Fellows will be selected in late 2020 and the Virtual Institute will commence in the spring.

2.10 Law and Policy Insights

Background. The IU Center for Applied Cybersecurity Research (CACR), which leads Trusted CI, maintains a student affiliate program with the Indiana University Maurer School of Law, wherein law students gain experience working with CACR's on-staff legal experts, including work on the Trusted CI Law and Policy Insights project. In 2020, the Law and Policy Insights project will focus on the development of in-depth guidance on particularly complex or salient issues facing the community: specifically, GDPR compliance and the Cybersecurity Maturity Model Certification (CMMC). These in-depth guidance materials will walk through the requirements in detail, providing more granular analysis of what those requirements mean and how to approach their implementation.

Progress this year. We engaged two students from the IU Maurer School of Law for Spring 2020 to conduct research relating to the European Union's General Data Protection Regulation and the US Department of Defense's Cybersecurity Maturity Model Certification (CMMC).

We received final research memos from the two IU Maurer School of Law student affiliates relating to the European Union's General Data Protection Regulation (GDPR) and the US Department of Defense's Cybersecurity Maturity Model Certification (CMMC). We began work on a final deliverable providing generalized guidance on GDPR's requirements for data controllers and processors.

We developed and presented a training lecture on US cybersecurity regulations, compliance, and CMMC. We onboarded a Student Affiliate for the Fall 2020 semester, who will be assisting with the development of the GDPR guidance document.

Plans for next year. We will present the CMMC lecture for the Trusted CI Webinar series in October 2020 and will finalize development of the GDPR guidance document.

2.11 Quilt Collaboration

Background. A new activity for 2020, the goal of this project is to leverage a collaboration with the Quilt[38] and Research and Education Networks (RENs) across the U.S. to broadly disseminate Trusted CI training. In 2020, the inaugural year of this effort, the goal is to produce and disseminate some initial training material to RENs at the Fall Quilt Member Meeting and begin the process of supporting those RENs in providing that training to their membership, which will carry over into 2021.

Progress this year. After reviewing the topic survey of the RENs at the Fall 2019 Quilt Meeting, Trusted CI presented the results at the 2020 Quilt Winter member meeting Feb 5-7. The initial topic was chosen to be "Information Security and Research Computing Collaboration" based on a previous Trusted CI and Internet2 collaborative workshop held at the Fall 2018 Quilt meeting.

Trusted CI held several discussions with interested Regional Network representatives to understand how they may provide training to their membership and how to provide training to them that would be most beneficial to them and their members. There is great diversity in how each Regional Network operates, what services they provide to their members, and variety in whether they are engaged with the research computing and security professionals at their member campuses. These discussions revealed that the regional network's primary engagements with their member campuses are through the networking groups and CIOs and very few were engaged with the research computing and security groups.

The pandemic impacted the community's capacity to both hold meetings and create plans, so our discussions evolved into how to best approach our goals of scaling the impact of Trusted CI broadly under the current circumstances. The Trusted CI Team has continued meetings with Quilt Executive Director Jen Leasure as well as group and individual discussions with multiple regional network leaders.

Plans for next year. Trusted CI will continue to engage with Quilt members to evaluate the feasibility of having a virtual workshop in the spring of 2021, still roughly based on the workshop held at the 2018 Quilt workshop. Each regional representative would be assisted in forming a team or two of participants from their members that includes research computing

[38] https://www.thequilt.net/

and security professionals to promote and enrich these partnerships to improve trustworthiness of cyberinfrastructure by implementing practices recommended by Trusted CI. The participants will commit to meeting with their team at least once prior to the workshop and then share their understanding and experiences of security practices suited to supporting science.

2.12 Annual Challenge

Background. Starting in 2020, Trusted CI is annually addressing a cybersecurity challenge to reproducible, trustworthy science that is unlikely to be addressed without our leadership and a sustained focus over a year. Our challenge for 2020 is the issue of data integrity. As called out in the Federal Cybersecurity R&D Strategic Plan, "In many situations, integrity and availability are the dominant properties of interest," and data integrity is a particular challenge for trustworthy, reproducible science as large data sizes are surpassing protections in our current IT infrastructure. Data integrity is also not well addressed in many cybersecurity control sets (e.g., NIST 800-171 is focused on confidentiality). Some science projects already undertake their own data integrity protections, but there is no community consensus on the risks to scientific results or guidance to projects for protecting integrity. This makes a consensus for data integrity critical, particularly as data infrastructure is growing ("Harnessing the Data Revolution" is one of the NSF's 10 Big Ideas).

Progress this year. We have formed the Trustworthy Data Working Group[39], a collaborative effort of Trusted CI, the four NSF Big Data Innovation Hubs[40], the NSF CI CoE Pilot[41], the Ostrom Workshop on Data Management and Information Governance[42], the NSF Engagement and Performance Operations Center[43] (EPOC), the Indiana Geological and Water Survey[44], the Open Storage Network[45], and other interested community members. The goal of the working group is to understand scientific data security concerns and provide guidance on ensuring the trustworthiness of data. To better understand scientific data security concerns, the working group conducted a community survey. Our survey report[46] analyzes the 111 survey responses that we received from respondents in a wide range of positions and roles within their organizations and projects. Then, the working group drafted guidance, shaped by the results of the survey, on trustworthy data for science projects and cyberinfrastructure developers. This guidance addresses attributes of trustworthiness, barriers to trustworthiness, tools and technologies for achieving trustworthiness, and methods for communicating trustworthiness.

[39] https://trustedci.org/trustworthy-data
[40] https://www.bigdatahubs.org
[41] https://cicoe-pilot.org
[42] https://ostromworkshop.indiana.edu/research/data-management
[43] https://epoc.global
[44] https://igws.indiana.edu
[45] https://www.openstoragenetwork.org
[46] https://doi.org/10.5281/zenodo.3906865

Metrics. The working group currently has 56 members. The survey report has 257 downloads.

Plans for next year. The working group will publish a draft of its community guidance at the end of September 2020, then solicit community feedback through various outreach channels, and revise the community guidance based on that input, for final publication in December 2020. Publishing the community guidance will be the final activity of the working group, thus completing the Annual Challenge for 2020. The Annual Challenge topic for 2021 will be Software Assurance.

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 those projects with tackling their specific challenges with cybersecurity in the support of NSF science.

3.1 Engagement Applications

Background. Trusted CI directly supports individual NSF cyberinfrastructure projects and Major Facilities through collaborative engagements that address specific project needs. Trusted CI engagement activities include (but are not limited to) security reviews, security architecture design, identity and access management, and software assurance. Twice per year, we open up a call for engagement applications. Once the application period closes, our leadership team convenes to review the applications and select engagees for the next engagement period.

Progress this year. In 1Q2020, we opened and publicized a call for applications for engagements to be executed in the second half of 2020 (see subsequent engagement reports below). We received 7 applications and selected the following engagements:

- Galaxy
- UNAVCO
- SCiMMA
- SOCCOM

In 3Q2020, we opened and publicized a call for applications for engagements to be executed in early 2021. As of September 8th, we have received 1 application. As the deadline for applications is October 2nd, we expect to receive more applications.

Plans for next year. We will open the engagement application period in February 2021 for engagements to be executed in the second half of 2021. We will also open the engagement application period in August 2021 for engagements commencing in 2022.

3.2 Engagement Success Stories

This year, in addition to conducting our post-engagement surveys, we onboarded team members from Indiana University's IT Communications team to reach out to prior engagees to assess the long-term impact of their engagement. The goal is to provide Trusted CI with valuable feedback and also increase our outreach to the community and encourage future engagements. These will be published to the Trusted CI website and blog.[47]

We will soon be releasing a success story summarizing the impacts of the Trusted CI engagement on the Academic Research Fleet. As a result of their engagement with us, they were able to secure additional funding to develop their Cybersecurity Pilot Program, which will include a plan for IMO and DFARS requirements.

3.3 Consultations

Background. In addition to engagements, another way we serve the community is through 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.

Progress this year.

- In early March, HPC labs Chameleon and Cloudlab became aware of an incident where attackers were able to gain access to computing resources in their facilities to mine cryptocurrency by using a federated identity from another HPC facility. Administrators from Chameleon and Cloudlab reached out to Trusted CI for advice. The IdM working group, along with several Trusted CI staff, helped those administrators to draft and send an announcement about the incident to the Federated Identity Discussion list on Trusted CI. The IDM working group also helped to coordinate information sharing regarding the incident with staff at NCSA and Open Science Grid.
- Anurag Shankar provided consulting and direction to the Galaxy team wishing to establish a commercial instance of Galaxy that is SOC2 compliant.
- We received confirmation from a prior engagee, the Academic Research Fleet, that they were able to secure additional funding as a result of our engagement report delivered in 2019.
- At PEARC2020, Mark Krenz met with a medical researcher at University of Michigan and provided her with information resources about protecting web applications.
- Provided guidance to University of Arizona on issues related to research computing with regulated data, such as secure enclaves in the cloud to address cybersecurity and compliance terms in grants, contracts, and data use agreements.

[47] https://www.trustedci.org/successstories

- Provided guidance to a team from the Miami-Dade Beacon Council, University of Miami, and Florida International University on starting a regional cybersecurity effort.
- In response to our offer to provide emergency consultation for projects dealing with issues related to the COVID-19 pandemic and the quarantine, Mark Krenz provided security advice and input to a visualization lab at UCLA that was trying to implement a remote render farm for students.
- We met with the Open OnDemand team[48] regarding increasing queries they are receiving with regard to their secure development practices. We expect this will translate into an engagement application for 2021.

3.4 Franklin and Marshall

Background. Franklin and Marshall is a private liberal arts college in eastern Pennsylvania. In 2019 they applied for an engagement with Trusted CI to help them enhance their existing cybersecurity program to better prepare for new NSF grants in computing. After kicking off the engagement in December 2019, they quickly realized that the engagement process would require more time than they expected and expressed a desire to pull out of the engagement. The Trusted CI team was very interested in pursuing this engagement and offered to scale down the engagement or do a cyber checkup, but F&M unfortunately had to decline and let us know that they would reapply for an engagement in the future when they are ready. The Trusted CI staff time that was previously allocated to this engagement was reallocated to other projects including Project X, which is covered under the Broader Impacts section (2.8).

3.5 Galaxy

Background. Galaxy is an open-source, web-based application for performing data-intensive biomedical research. It combines common software tools and data workflows to provide researchers without an informatics platform an accessible, easy to use interface, which abstracts the complexity of interacting with compute resources. Galaxy applied for an engagement with Trusted CI in the first half of 2020. The primary focus of this engagement is to review the Galaxy docker container deployment model to check its alignment with NIST 800-53 and provide a gap analysis in order to recommend tools and controls. This engagement is scheduled to conclude in December 2020.

Progress this year. The Trusted CI team has guided the Galaxy team in creating detailed architecture diagrams for all user and administrative processes in order to best understand the possible flows of data on the system. Trusted CI is currently following the 800-53 SSP process.

[48] https://openondemand.org/

Plans for next year. We plan to finish the NIST 800-53 SSP process, then analyze gaps between existing controls and suggested controls. Then we will provide a report to the Galaxy team containing these recommendations.

3.6 Globus Auth

Background. 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. While there are no public version numbers for Globus Auth, the software that we assessed was published in 2019-08-23 and was running in production from 2019-08-21 until 2019-09-11. The git tag was “release/production/2019-08-21.0”. This software was given to the Trusted CI team packed in Docker containers that differ from the production environment in the Amazon cloud.

Progress this year. After applying the five steps of FPVA, in July 2020 we completed the final engagement report and shared it with the Globus team. The report is now publicly shared.[49] Overall, our team found no security issues in the Globus Auth code, however we made several recommendations to further increase security based on findings from our assessment.

3.7 Open Storage Network

Background. The Open Storage Network (OSN)[50] is an NSF-funded pilot project (OAC 1747483, 1747490, 1747493, 1747507, and 1747552). The OSN pilot project's goal is to design and test a cooperative multi-institution, research-oriented storage and transfer service, including a governance model to manage both the technical system and user allocations. The outcome of the pilot project will direct the design of a national scale infrastructure that can serve as a storage substrate along with NSF's other national investments (e.g., XSEDE) and network implementations supported by NSF's CC* program.

Progress this year. OSN staff first used Trusted CI's "Securing Commodity IT in Scientific CI Projects" spreadsheet[51] to evaluate five facilities including NCSA, SDSC, RENCI, MGHPCC, and JHU. These results were then used to evaluate the OSN system as a whole. OSN staff next completed Trusted CI's "Information Security Program Evaluation" questionnaire[52]. This document was used to capture the current state of the OSN information security program as well as find potential security policy gaps in the pilot program. The output from these CyberCheckup documents will be used by OSN to better secure future phases of the project.

[49] https://www.ideals.illinois.edu/handle/2142/106617
[50] https://www.openstoragenetwork.org/
[51] https://docs.google.com/spreadsheets/d/12Tad4eK4k9OLfMjv1N70iughbx-kNwQRKh6Y3CfHBpI/edit
[52] https://bit.ly/2OgVAr6

3.8 Scalable Cyberinfrastructure to Support Multi-Messenger Astrophysics (SCiMMA)

Background. The Scalable Cyberinfrastructure Institute for Multi-Messenger Astrophysics (SCiMMA), funded under NSF grant #1934752, is a planned collaboration between data scientists, computer scientists, astronomers, astro-particle physicists, and gravitational wave physicists. Leveraging NSF investments in astronomical and multi-messenger facilities and in advanced cyberinfrastructure, SCiMMA intends to prototype a publish-subscribe system based on Apache Kafka to distribute alerts from gravitational wave, neutrino and electromagnetic observatories to authorized subscribers (initially, public alerts so that all subscribers are authorized, but eventually proprietary alerts). The system will additionally rely on supporting infrastructure, including: machine learning algorithms to analyze and classify alerts; an AARC2-style federated identity and access management suite; and event databases for richer data mining. The pub/sub prototype will be hosted on cloud resources, including a commercial cloud. Upon award completion, SCiMMA will pursue funding for a sustained distributed institute that will expand the scope and depth of the prototyped system.

To this end, SCiMMA is seeking help on and-or with various components of their prototype cyberinfrastructure. Primarily, they seek to develop a sound IT security program. Through a kick-off meeting and post-discussion, Trusted CI and SCiMMA have defined and prioritized their needs using a subset of tasks, outlining the goals of the engagement, specifically:

1. Perform a security review of SCiMMA's cyberinfrastructure using the Trusted CI Security Program Evaluation worksheet in order to assess the target level of cybersecurity needed;
2. Using information documented in step 1, develop the start of a security program leveraging a master information security policies and procedures document;
3. Develop an asset inventory to be used by the security program in step 2, and;
4. Perform a nascent risk assessment using identified assets with a corresponding residual risk registry.

Upon completion of the engagement, Trusted CI will produce a final, publishable report describing the work performed, potential impact to the open-science community, and areas SCiMMA may find appropriate for future engagements.

Progress this year. We guided SCiMMA through our Security Program Evaluation and have begun developing their asset inventory and asset-based risk assessment.

Plans for next year. In 4Q2020, we expect to develop and complete a security program that leverages the asset inventory and risk assessment performed in the 3Q2020 of the engagement.

3.9 Southern Ocean Carbon and Climate Observations and Modeling (SOCCOM)

Background. The SOCCOM[53] project is a $21 million project to instrument the Southern Ocean and make data publicly available. SOCCOM has deployed nearly 200 robotic profiling floats in the Southern Ocean (south of 30oS). These floats are part of the international Argo network and collect physical, chemical, and biological sensor data from the upper 2000 m of the water column every 10 days. The data are transmitted to shore via the Iridium satellite system. The data are then passed through a series of institutional servers, where the data are fully processed and quality controlled. The resulting science quality data and the raw observations are made available within 24 hours with no restrictions. The data set has been used in more than 100 publications to assess physical, chemical, and biological processes in the Southern Ocean.

Progress this year. SOCCOM filled out the information security program evaluation and Securing Commodity IT in Scientific CI Projects: Baseline Controls and Best Practices. Using these documents, the SOCCOM project was able to identify their security footing for members of the SOCCOM project, including MBARI, Woods Hole Oceanographic Institute, Scripps Institute of Oceanography, and the University of Washington. In addition this brought up questions of common solutions and problems each group faces. These were accomplished through monthly zoom calls. In the September monthly call the group met with Craig Jackson to discuss Information Security Program development and governance.

3.10 UC Berkeley (UCB) Secure Research Data and Compute (SRDC)

Background. UCB is building the SRDC Platform to handle restricted research data on campus. SRDC is funded by UCB executive leadership as a condo-style research computing service. This institutionally supported foundation for restricted data research will be professionally managed and supported by Research IT staff from UCB and Lawrence Berkeley National Lab, and researchers will contribute computation and storage hardware to the platform using their research funds. The SRDC Platform will bring together HPC nodes, virtual machines, and big data storage for researchers working with highly sensitive data (e.g., PHI and PII) across a range of domains, many of which are NSF-funded. To help UCB achieve this goal, we will review UCB's design of the SRDC environment, provide feedback, and recommend strategies to protect sensitive data.

[53] https://soccom.princeton.edu

Progress this year. We collected and reviewed artifacts that highlighted various aspects of the UCB vision and held weekly meetings with UCB personnel and internal meetings to supplement our understanding of both existing practices and the proposed approach to SRDC. We also conducted a day-long virtual visit of UCB where we met with many stakeholders such as the UCB Information Security Office, central IT, and HIPAA officers and did a presentation to apprise them of how peers are approaching the regulated data challenge.

We completed the engagement and delivered the final report with recommendations to UCB. A blog post covering the successful completion was posted to the Trusted CI blog and the engagement was the subject of our first Engagement Success Story[54]. A post-assessment survey was completed, indicating a high level of satisfaction by UCB.

3.11 UNAVCO/GAGE

Background. GAGE is a distributed, multi-user, national facility for the development, deployment, and operational support of modern geodetic instrumentation to serve national goals in basic research and education in Earth Sciences. The CI CoE Pilot team began an engagement with GAGE in July to improve the state of Identity Management (IdM) practice and infrastructure by producing a plan and proof of concept for a new IdM solution to facilitate external users to access GAGE's research data and providing GAGE with a means of tracking who is using accessing their data by using federated identities provided by Incommon member institutions and third party commercial identity providers.

Progress this year. The CI CoE Pilot Identity Management working group began meeting with GAGE in July and conducted a series of interviews with GAGE leadership and key personnel to build an accurate picture of the current state of IdM in GAGE and assess future needs. In September, the IdM team began meeting with GAGE technical personnel to implement a proof of concept IdM solution utilizing CILogon, COManage, and OAuth2/OIDC to consume external federated identity sources, assign GAGE specific attributes to those identities using COMangage and provide OIDC tokens to a GAGE web application, allowing users to access GAGE's research data, and allowing GAGE to associate digital identities with each data access.

Plans for the next year. The proof of concept solution and final report will be delivered by February 2021.

3.12 XSEDE Metric Service

Background. At the end of March, we started an in-depth vulnerability assessment of XSEDE Metric Service (XDMoD). XDMoD is an open source tool to manage high performance computing resources. Open XDMoD's management capabilities include monitoring standard

[54] https://www.trustedci.org/s/Trusted-CI-Success-Story-UC-Berkeley.pdf

metrics such as utilization, providing quality of service metrics designed to identify underperforming system hardware and software, and report job level performance data for every job running on the HPC system without the need to recompile application[55].

The primary goal of the XSEDE Metrics Service engagement is to review the software and to help ensure its design and implementation are secure - that is, it is free of design errors and will function as intended in the face of malicious entities attempting to coerce it to do otherwise.

Progress this year. We studied the basic functionality of the XDMoD application and applied the five steps of the First Principles Vulnerability Assessment (FPVA) methodology. We generated the architectural and resource diagrams, including privilege information. We also analysed the code in depth and found three significant security vulnerabilities, writing reports for each of these vulnerabilities and delivered them to Ryan Rathsam, our contact for this engagement. We wrote and delivered the engagement final report, which will be publicly available in February 2021.

The first vulnerability that we found in XDMoD is the use of HTTPS (vs. HTTP) is not mandatory. Communicating over unencrypted channels exposes all information sent between the client and the server, including cookies and passwords. Second, Open XDMoD was found to be logging sensitive information to a globally readable file. Third, a DoS attack was possible by filling all the free space on a disk partition containing Open XDMoD's log files, causing the web portal to become inoperable. Additionally, the assessment found that OpenXDMoD relies on three software dependencies that are either unmaintained or out of date.

Plans for next year. The engagement final report will be publicly available in February 2021.

4 Engagement Evaluations

Background. Since August 2016 we have routinely followed up with prior engagements to assess long-term impact and our own engagement processes. We have received 33 responses to our Engagement Evaluation Questionnaire[56] to date, including 2 responses in 2020. 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 29 of 33 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.

[55] https://open.xdmod.org/8.5/
[56] https://goo.gl/forms/VHL8Gtda2nWMgu9H3

However, not every response indicates maximum positive impact. Several respondents identified barriers to the engagement having more positive impact, mostly commonly selecting "Other priorities diverted attention from cybersecurity" and "Insufficient staff/budget/resources to make recommended changes." The 2020 responses indicate that these barriers are less prevalent than they have historically been and that the COVID-19 pandemic posed an unexpected barrier for our engagees.

The 33 responses include 24 first time evaluations, 5 first follow-up evaluations, and 4 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 33 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.

21 of 32 responses were 5. All 32 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 of the 33 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.

The most frequently selected responses were:

- Knowledge / documentation of information assets (22)
- Increased cybersecurity knowledge among staff and personnel (20)
- Understanding cybersecurity risks to the science mission (19)
- Improved governance / policy / risk acceptance structure (19)
- Communication of risks to decision-makers and stakeholders (18)

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" and "understanding cybersecurity risks to the science mission"

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."
- 1 response indicated challenges created by the COVID-19 pandemic

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)

29 of 33 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 9 ratings of 5. 32 of 33 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"; 11 of "somewhat better"; 5 of "about the same".
- **Quality of communication**. 21 ratings of "much better"; 7 of "somewhat better"; 4 of "about the same".
- **Quality of deliverables**. 16 ratings of "much better"; 12 of "somewhat better"; 4 of "about the same".
- **Positive impact on security**. 16 ratings of "much better"; 8 of "somewhat better"; 7 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.

21 of 29 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 26 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?

17 of the 25 responses had useful and constructive feedback on our processes. 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 verbatim survey 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 Program Administration

Background. This section summarizes the administrative activities we complete in support of Trusted CI and the team generally. This includes, but is not limited to:

- Project reporting/tracking via project plans;
- Effort allocation and management;
- Facilitating recurring meetings and the annual all hands meeting;
- Engagement with the Advisory Committee (AC);
- Budgeting/overseeing spending;
- Establishing program templates, policies, and procedures;
- And reporting.

We allocate one hour/week for each staff member to support these activities. Staff with leadership roles have larger allocations.

Progress this year.

- The leadership team and project activity leads finalized effort allocation aligned to each activity for the first half of the calendar year.
- We modified our recurring meeting schedule to accommodate conflicts that arose for the semester and to align more closely with strategic goals and leadership roles.
- The leadership team and project activity leads finalized effort allocation aligned to each activity for the second half of the calendar year.
- We evolved our project reporting documentation and processes to allow for more rigorous evaluation of planned vs. actual progress.

Plans for next year. We will monitor our new meeting and reporting processes to ensure efficacy and will further refine if needed.

5.2 Advisory Committee Changes and Meeting

Background. The Trusted CI Advisory Committee serves to provide Trusted CI with strategic guidance. It is convened for an in-person meeting each year co-scheduled with the SuperComputing conference and consulted ad hoc throughout the year. The Trusted CI Advisory Committee members are as follows:

- Eric Cross, Information Technology Manager for the National Solar Observatory (NSO)
- Neil Chue Hong, Director of the Software Sustainability Institute (SSI)
- Damian Clarke, CIO at Alabama A&M
- Ewa Deelman, Research Professor of Computer Science and Principal Scientist at USC Information Sciences Institute, principle investigator of the CI CoE Pilot
- Anita Nikolich, Research Professor of Computer Science at Illinois Institute of Technology, Co-Director of FABRIC

- Michael Zentner, 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

Their bios can be found on the Trusted CI website[57].

Progress this year. Due to the COVID-19 pandemic, in collaboration with the Advisory Committee, we decided to shift the upcoming AC meeting to be a virtual event instead of on site at SC20.

In an effort to further balance the perspectives and experience represented by the Advisory Committee, Ewa Deelman, Anita Nikolich and Damian Clarke have agreed to join. Tom Barton and Nicholas Multari, both members of the AC since its inception, stepped off of the AC and receive our highest thanks for their contributions to Trusted CI.

Plans for next year. We will onboard our new AC members and convene the full group virtually on November 2 and 3.

5.3 Trusted CI All Hands Meeting

Background. Each year, we hold the Trusted CI all hands meeting which is an opportunity for all team members to come together for an in-person meeting to discuss project activities, strategic initiatives, and to brainstorm solutions for new and unique challenges.

Progress this year. The 2020 all hands meeting was held on March 3rd and 4th at the Big Ten Center in Rosemont, IL. All but one Trusted CI team member was present for the meetings. In addition to reviewing the status and plans for all of our activities, the team discussed:

- Opportunities to more effectively track our outreach to diverse and underrepresented populations while continuing to respect the privacy of the community.
- Providing more timely and frequent updates on new or changing activities.
- The leadership team providing monthly summaries of the outcomes of their weekly meetings at our monthly all hands calls.

Plans for next year. We will hold the 2021 all hands meeting in March, either in person or virtually (depending on appropriate safety protocol and institutional policies).

[57] https://trustedci.org/advisory-committee

5.4 Project Changes from the Project Execution Plan

Background. On December 20, 2019, we delivered the project execution plan (PEP) covering the period from January 1, 2020 to December 31, 2020 (offset from the official project year due to the spend down of prior grant funds in 4Q2019). The PEP included a summary of each major program activity, our expenditures plan, and the details of our program governance plan, including a change management plan. As part of our change management plan, we will communicate small changes to the project via our quarterly reports.

Changes this year.

- There was an error in section 8.1 of the PEP. We will deliver the 2Y1Q quarterly report by no later than the end of January 2021. (The report stated December 2020.)
- We consolidated leadership for the Framework project. Jim Basney's effort on the Framework decreased from .01 to .00; Von Welch's increased from .05 to .1 (with him assuming the lead role on advisory board governance).
- As discussed in Section 3.4, our Engagement with Franklin and Marshall do not go through as expected and we shifted that effort.
- We further increased Shane Filus' allocation on Trusted CI activities as his role expanded to accommodate a reduction in Andrew Adams' available time. Shane's allocations increased on: the SGCI collaboration and the CI vulnerability program.

Plans for next year. Prior to the end of 2020, we will update and expand the PEP to include the remaining award period (through 2024).

5.5 Personnel Changes

The team had the following personnel changes in the reporting period (January 2020 through September 2020):

- Carnegie Mellon University/PSC
    - Shane Filus, a Security Engineer at PSC, joined the team in January. He brings over 15 years of networking and security expertise to the SGCI and CI Vulnerability projects and the Trusted CI Security Program.
- University of Wisconsin-Madison.
    - Benjamin Kinzer left as he graduated in May 2020.
    - Ian Ruh joined the team as a student researcher at the University of Wisconsin-Madison in March 2020. Ian's time commitment is 20 hours per week after classes finish (since May 2020). Before that his time commitment was 5-10 hours per week. He contributed to the software assessment of XDMoD and report writing.

- Lawrence Berkeley National Lab
    - Jinyue Song, a PhD student at UC Davis, joined the team from June-September 2020 as a summer student.
    - Jason Lee, a security engineer at LBNL/NERSC, joined the team in August 2020 and brings decades of R&E networking, security, and HPC experience. His time commitment will be 4 hours per week.
- Indiana University/CACR
    - Adrian Crenshaw and Josh Drake joined the team as part of the CI CoE pilot collaboration team.
    - Ranson Ricks and Emily Adams joined and are on the Framework project team.
    - Julie Songer and Todd Stone, both of IU's IT Communications department, joined the team. Their focus has been on interviewing past Trusted CI engagees and assessing the long-term impact of the engagements.
    - Florence Hudson is departing the program on September 30, 2020. We have taken proactive action to onboard Ryan Kiser to the TTP effort and he will be leading it after Florence's departure.
- University of Illinois/NCSA and Internet2 experienced no staffing changes this year.

5.6 ResearchSOC Collaboration

Background. Trusted CI PI Welch also directs the ResearchSOC project[58], a collaborative security response center under CICI 18-547 (NSF award #1840034). While the two projects have distinct roles in the NSF ecosystem (Trusted CI is a trusted, technology-neutral cybersecurity leader and consultant, and the ResearchSOC is developing a set of operational cybersecurity services with a sustainability model of for-fee service), they regularly collaborate on the Situational Awareness service (see Section 2.2), their information security programs (see Section 5.8), and collaborate on outreach.

Progress this year. The EDUCAUSE Security Professionals Conference shift to an online event disrupted collaboration plans. At PEARC, Indiana University had a sponsorship table representing both projects. Two talks from ResearchSOC are part of the 2020 NSF Cybersecurity Summit program.

Plans for next year. Trusted CI will continue to collaborate on Situational Awareness, their information security programs, and outreach at PEARC, the NSF Cybersecurity Summit, and other events.

[58] https://researchsoc.iu.edu/

5.7 Sustainability

Background. Trusted CI is 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 the CI CoE in Section 1.6), and ultimately non-NSF projects when such support would not detract from our mission of supporting the NSF community and NSF science.

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

- CI Center of Excellence (CoE) Pilot (NSF award #1842042, PI Deelman): shared .5 FTE.
- Science Gateways Community Institute (SGCI, NSF award #1547611, PI Zenter): shared .5 FTE.
- Infrastructure for Privacy-assured CompuTations (ImPACT)[59] (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)[60]: $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[61].
- Professor Miller 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).
- Open Science Grid (OSG)[62]: A national, distributed computing partnership for data-intensive research (NSF award #1148698, PI Livny): .5 FTE to provide operational security support to the Open Science Grid.
- Institute for Research and Innovation in Software for High Energy Physics (IRIS-HEP, NSF award #1836650, PI Elmer): .5 FTE to provide operational security support to the OSG-LHC program.

[59] https://renci.org/impact/
[60] https://cacr.iu.edu/pact/
[61] https://indianavoters.in.gov/MVPHome/ElectionSecurity
[62] https://opensciencegrid.org/about/introduction/

- DHS funded Continuous Software Assurance through a National Marketplace (SWAMP)[63] (NSF award #, PI Livny): .5 FTE to provide operational cybersecurity support to the SWAMP (concluded in 2020).

Progress this year. CACR is part of the OSG team which received a renewal this year[64] and through the ResearchSOC, CACR is now providing cybersecurity support to the National Radio Astronomy Observatory (NRAO)[65]. CACR is also analyzing our current experiences, listed above, to structure our cybersecurity service offering and which are now reflected on the ResearchSOC website[66].

Plans for next year. We will complete the structuring of our cybersecurity services and advertise them on both the Trusted CI and CACR websites.

5.8 Trusted CI Cybersecurity Program

Background. Trusted CI maintains its own cybersecurity program, both to assure it facilitates secure handling of information data, as well as to show, by example, how NSF projects can use the tools Trusted CI provides in order to develop a cybersecurity program. The program has several responsibilities, including: developing and periodically updating policies that help guide Trusted CI personnel in performing Trusted CI's mission; mitigating and responding to incidents; monitoring and providing disaster recovery (DR), where possible, to Trusted CI assets; and staying abreast of current vulnerabilities and threats.

Progress this year. In response to Trusted CI experiencing their first incident (*Trusted CI Incident Response Report 2019-10-02_01*[67]), Trusted CI initiated a process to improve its own cybersecurity program based on information revealed during said incident's post-mortem.

We began development on a policy for Trusted CI's Google Drive file-store, including: labeling scheme for external sharing, backup & restore implementation(s) and testing, a tagging scheme to aid in automated detection of misshared documents, and ownership changes due to offboarding or role changes. The document labeling scheme was approved by leadership and implemented, and updates/enhancements were made to several of the policies.

Due to COVID-19, we spent considerable effort in understanding threats and mitigations posed by remote work[68]. The most notable of these was the conferencing application Zoom. We relayed pertinent information regarding Zoom as a 'security best practices' guide to not only

[63] https://continuousassurance.org/about-us/partners/
[64] NSF award 2030508
[65] https://itnews.iu.edu/articles/2020/Keeping-mysteries-universe-safe-from-hackers-.php
[66] https://researchsoc.iu.edu/services/proposals.html
[67] http://hdl.handle.net/2022/24845
[68] https://blog.trustedci.org/2020/03/recommendations-for-reducing.html

Trusted CI personnel but also to our community[69]. Additional tasks addressed during 1-3Q2020 include:

- Publishing the incident response report for the community to experience.
- Creating a document labeling scheme specifically for Trusted CI to mitigate against similar breaches from occuring in the future.
- Re-designing and developing a new Incident Response policy.
- Undertaking the process of periodic table-top exercises.
- Instantiating a (cloud-based) ticketing system to be used for security incidents and maintenance (e.g., onboarding, offboarding, periodic reviews, and table-top exercises).
- Applying updates the Master Information Security Policies & Procedures.
- Continuing development on the Google Drive file-store policy.
- Creating a Google Drive document filename tagging scheme to allow for easier detection of files whose sharing settings are not as intended.
- Initiating work on drafting onboarding & offboarding policies.

Plans for next year. We will continue to execute Trusted CI's security program, updating/enhancing policy & procedures, as necessary, and engaging in maintenance security tasks.

6 International Travel and Impact

During project year one, the Trusted CI team undertook no international travel under Trusted CI funding.

7 Metrics

Table 7. Trusted CI activity goals and achieved metrics.

Activity	Measurement Technique	Goals	Achieved
Engagements with NSF projects.	Direct measurement of the number of engagements.	4-6/year depending on complexity.	On track. Six engagements completed in 2020 (Galaxy, Open Storage Network, SCIMMA, SOCCOM, UC Berkeley, XSEDE Metrics Service)
	Post-engagement survey.	High ratings of engagement utility.	On track. See Section 4 for new results.
	Consultations (new)	None.	6 (see Section 3.2)

[69] https://blog.trustedci.org/2020/04/the-extra-zoom-setting-you-may-not-know_8.html

Table 7 (continued). Trusted CI activity goals and achieved metrics.

Activity	Measurement Technique	Goals	Achieved
NSF projects using our best practices, guides, threat model to develop and maintain their own cybersecurity programs.	Reported by NSF projects.	Initially 2-4/year using cybersecurity program guide. Aim to increase linearly.	The NSF Community Cybersecurity Benchmarking Survey performed by Trusted CI identified in 2020 that 5 projects are using the Trusted CI guide.
Cyberinfrastructure Vulnerabilities / *Situational Awareness*	Direct measurement of number of individuals and NSF projects receiving announcements.	Aim to increase the number of individuals subscribed each year.	Currently 159 subscribers on the situational awareness list.
Training	Direct measurement of attendance.	50 members of NSF community per year attending.	Training on "Web security and Automated Assessment Tools" will be presented at NSF Cybersecurity Summit 2020 Training on "Web Programming and Automated Assessment Tools" to be presented at Gateways 2020 Training on "Secure Programming and Automated Assessment Tools" to be presented at Supercomputing 2020
	Survey of attendees.	100% rating training as valuable.	Surveys results will be published in the 2021 Annual Report.
Summit	Direct measurement of attendance.	90%+ participation of Large Facilities. Strong, diverse participation across the full range of NSF CI projects, and program officers.	Representation from 87 NSF-funded projects in the 2020 Summit including 15 large facilities registered as of September 8th.
	CFP response rate.	Increasing CFP response rate each year.	There were 22 responses to the CFPs in 2020.
	Surveys of attendees.	Very strong evaluations on attendee surveys.	A post summit survey results will be presented in the 2021 annual report.

Table 7 (continued). Trusted CI activity goals and achieved metrics.

Activity	Measurement Technique	Goals	Achieved
Software Assurance	Post-engagement assurance tool usage by projects, on 3, 6 and 12 month time scale	Linear progression each year on tool use.	Nothing to report yet.
	Number of projects that engage us for the Moderate and Deep Dive levels.	3-4 requests for engagements each year.	In our two engagement application cycles in 2020, 2 applicants requested software assessments.
	Number of individuals using online training materials	Linear progression each year.	4118 views.

Table 7 (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. Presented: "Trusted CI: Cybersecurity for Productive, Trustworthy, Reproducible Science" at the National Science Foundation "The Mission of Cybersecurity in Science: Productivity, Reproducibility, and Trust" at the SIAM Minisymposium on Transparency, Reproducibility, Sustainability, and Security: The Four Pillars of the Next Generation Scientific Software Stack Town hall presentation regarding COVID-19 impacts on the NSF open science community Presentation on the BDHubs Data sharing and CI Working Group Call Presented at the Educause Security Professional Conference on the Department of Defense's Cybersecurity Maturity Model Certification (CMMC) Workshop on Trustworthy Scientific Cyberinfrastructure, "PEARC '20
	Mentions in NSF Solicitations	Goal is all solicitations with a requirement for a cybersecurity program to mention us as a resource.	2: Dear Colleague Letter: Cyberinfrastructure Centers of Excellence, Cyberinfrastructure Centers of Excellence (CI CoE)
	Webinar attendance and views of archives (new)	Continued growth	Attendance: 393 Archive views: 1,179 Yearly NSF Project Impact: 51
	Subscribers to Trusted CI email Lists (new)	Continued growth	Announce: 936 (+92 since 2019) Discuss: 629 (+95 since 2019)
	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 8. All Trusted CI Engagements (in progress and completed) under current award

Engaged Project	NSF Award # or Category	Engagement Subject
Franklin and Marshall	N/A	N/A: see section 3.5
Galaxy	NSF 1661497 and 1929694	Assess Galaxy docker deployment model's readiness for compliance with 800-53 and HIPAA and provide security recommendations.
Open Storage Network	IIS 1747552, 1747493, 1747507, 1747490, 1747483)	CyberCheckup, engagee-driven self-evaluation of the project's cybersecurity readiness
Scalable Cyberinfrastructure to support Multi-Messenger Astrophysics (SCiMMA)	OAC-1841625, OAC-1934752	Perform a CyberCheckup to review state of proposed architecture and development nascent security program
Southern Ocean Carbon and Climate Observations and Modeling (SOCCOM)	NSF 1936222 and 1425919	Perform a CyberCheckup, engagee-driven self evaluation of the project's cybersecurity readiness.
UC Berkeley Secure Research Data and Compute (SRDC) Platform	N/A	Guiding the design and implementation of the SRDC Platform and a procedural framework that maintains a healthy balance between usability and security
UNAVCO	1724794, 1851159, 1851163, 1851169	Assisting in implementing an identity management system for tracking use of data from research portal.
XSEDE Metric Service	OAC-1445806	Assessment of the security of the XSEDE Metrics Service, Open XDMoD, an open source tool to manage high performance computing resources.

Table 9. All Trusted CI Engagements under prior award (1547272)

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.

Table 9 (continued). All Trusted CI Engagements under prior award (1547272)

Engaged Project	NSF Award # or Category	Engagement Subject
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.
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

Table 9 (continued). All Trusted CI Engagements under prior award (1547272)

Engaged Project	NSF Award # or Category	Engagement Subject
Image Based Ecological Information System	1550881	Developed a role-based access control (RBAC) prototype. Goal was to establish an RBAC design to support the variety of image gathering, curation, and analysis workflows across multiple ecological communities.
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 9 (continued). All Trusted CI Engagements under prior award (1547272)

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.
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	Assistance in developing an information security program. Quick evaluation of information security program with recommendations for improvement. Training for staff.
XSEDE Metric Service	OAC-1445806	In-depth vulnerability assessment of XDMoD.

Table 10. CTSC (Trusted CI) Engagements under prior award (1234408)

Engaged Project	NSF Award # or Category	Engagement Subject
perfSONAR	Extensively used by R&E community and numerous CC-NIE awardees	Reviewed vulnerability management practices and performed code review of bandwidth controller (BWCTL)
AARC	EU Project	Collaborated to gather input from US cyberinfrastructure projects on AARClead activities, disseminate training and other AARC project outputs to US cyberinfrastructure projects, and facilitate EUUS pilot project activities.
HUBzero (2014-15)	Used by multiple NSF projects.	Review of Web Server Security Model and Disaster Recovery Plan documents.
OOI	Large Facility	Assisted in developing cybersecurity program.
LSST	Large Facility	Assisted in developing cybersecurity program.
NEON	Large Facility	Performed cybersecurity risk assessment on the NEON network of sensors and data servers.
CC-NIE (U. Cincinnati & U. Pittsburgh)	1440646 and 1541410	Facilitated peer-to-peer review of cybersecurity programs.
CC-NIE (U. Oklahoma)	1341028	Cybersecurity program review and guidance. Determined engagement was too early and suspended.
NTP	Core Internet infrastructure	Assisted in migration of source code to open source repository, modernization of build and test infrastructure, creating documentation suitable for onboarding new developers, and pruning old code.
DKIST	Large Facility	Assisted in development of a cybersecurity program. Cybersecurity Program Guide was key output.
Globus	Used by many NSF projects.	Conducted cybersecurity review of the architecture and design of the new sharing functionality.
CC-NIE (Penn State and U. Utah)	1245980 and 1341034	Facilitated peer-to-peer review of cybersecurity programs.

Table 10 (continued). CTSC (Trusted CI) Engagements under prior award (1234408)

Engaged Project	NSF Award # or Category	Engagement Subject
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.