Annual Report for 2021/ Project Year 2

Trusted CI
The NSF Cybersecurity Center of Excellence

NSF Grant ACI-1920430

October 1, 2020 - June 30, 2021[1]

For Public Distribution

Trusted CI Team

Ishan Abhinit[2], Andrew Adams[1], Emily Adams[2], Kay Avila[3], Jim Basney[3] (co-PI), Ritvik Bhawnani[4], 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], Elisa Heymann[4], Craig Jackson[2], 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], Julie Songer[2], Susan Sons[2], Todd Stone[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

[1] This annual report does not cover a full project year. This adjustment to the reporting schedule was made to enable a thorough NSF review and approval period and timely release of subsequent year funds.

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 the first three quarters of project year 2 (PY2) of Trusted CI under NSF grant 1920430. Prior to grant 1920430, Trusted CI was supported under NSF grants 1547272 and 1234408.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Please cite this report as:

> Trusted CI Annual Report for Project Year 2. July 2021.
> http://hdl.handle.net/2022/26651

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

Trusted CI PY2 Highlights

A. We released version 1 of the Trusted CI Framework Implementation Guide for Research Cyberinfrastructure Operators. The guide was downloaded more than 500 times during the first month and is being used in an engagement with NOIRLAB to assist the organization in adopting and aligning to the Framework.

B. Trusted CI completed engagements with Galaxy, SCiMMA, SOCCOM, FABRIC, PATh, Open OnDemand, and Michigan State University. We selected four engagements to be completed in the second half of 2021: University of Arkansas, Jupyter, OOI, and Ohio Supercomputer Center.

C. The 2020 NSF Summit report was published, summarizing the eighth annual Summit[2] organized by Trusted CI and the first to be held entirely online.

D. The CI CoE pilot collaboration team completed an engagement with the Academic Research Fleet and delivered a final engagement report.

E. The CI vulnerability team discussed 32 critical vulnerabilities and communicated a total of 14.

F. We interviewed six projects developing software for scientific computing and cyberinfrastructure in support of the 2021 Annual Challenge. The Challenge is focused on improving the robustness of software used in scientific computing with respect to security.

G. The presenters of “Making Identity Assurance and Authentication Strength Work for Federated Infrastructures” at the International Symposium on Grids & Clouds acknowledged use of the Open Science Cyber Risk Profile in their presentation and paper. In particular, they made use of the section on asset classification.

H. We evaluated 25 applications for the 2021 Fellows program and selected 8[3] to participate in this year’s program. We began the virtual institute in March.

[2] https://www.trustedci.org/2020-nsf-summit/

[3] https://www.trustedci.org/2021-fellows

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 2021, we will organize and host the NSF Cybersecurity Summit, which we have been hosting since 2013. The Summit brings together leaders in NSF cyberinfrastructure and cybersecurity to continue building a trusting, collaborative community addressing the community's core cybersecurity challenges.

Progress this year. We concluded activities for the 2020 NSF Summit by publishing our report summarizing the online event.[4] We transitioned into planning the 2021 Summit. The Trusted CI leadership team and organizing committee have discussed the potential implications of the COVID-19 pandemic on hosting an on-site event and expected reduction in available travel funding and elected to proceed with planning a virtual summit again this year.

We convened the program committee, consisting of members from higher education and NSF large facilities. Jim Marsteller will serve as the program committee chair and Anita Nikolich will serve as co-chair. We will take advantage of the online format by opening the plenary to the public. The workshops will be limited to community members and the presenters will establish criteria by which people are able to attend. This year's event will be held Oct. 11-15, with plenary talks on Oct. 12 and 13 and training and workshops on the other days. We opened the call for presentations.

Plans for next year. The program and organizing committees will evaluate CFP submissions, select the keynote, workshops, and plenary talks, and establish the Summit agenda.

1.2 Large Facility (LF) Outreach

Background. Since January 2017, Trusted CI has convened a working group for information security staff members at NSF's large facilities (LFs). This working group, the Large Facilities Security Team (LFST)[5], 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. The LFST 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.

[4] https://www.ideals.illinois.edu/handle/2142/108907

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

Progress this year. Trusted CI hosted eight calls in LFST's monthly conference call series with subjects chosen based on the Trusted CI Framework, trending cybersecurity challenges and topics, and member input. Topics covered in this reporting period included:

- Governance with regard to Cybersecurity Lead Reporting (Framework context)
- Supply Chain Vulnerability
- Operational Cybersecurity: working proactively to improve an organization's cybersecurity posture aligned with its resources and mission
- Site Access Challenges (multiple calls)
    - Identity and Access Management
    - Endpoint Security Management and Zero Trust Architecture
    - Challenges of supporting an increased remote workforce as a result of COVID

Two LFST member suggestions arose in the previous quarter:

1. Creating a forum for the sharing of attack/threat information between the LFST members, and;
2. Identifying Trusted CI resources to help LFSTs with Identity Management (IdM) challenges.

Trusted CI has begun taking steps to respond by exploring opportunities to collaborate with the ResearchSOC[6] (threat sharing and operational cybersecurity) and the CI CoE Pilot Identity Management Working Group (IdM WG) to make their expertise available to the LFST.

We continued quarterly communication with NSF's Large Facilities Office. Highlights were announcing availability of the 2020 NSF Cybersecurity Summit Report and scheduling of the 2021 Summit and providing feedback on the G*uidelines For Cyber-security of NSF's Major Facilities* section of the *NSF Major Facilities Guide* December 2020 draft.

Metrics.

- *Monthly calls:* LFST calls were held in October and December of 2020 and January through June of 2021. Average attendance by non-Trusted CI personnel was eight LFST members.
- *LFST site representation:* All LFs are represented directly or through their subprogram(s).

Plans for next year. Trusted CI plans to reevaluate, and potentially refocus and reprioritize, our LFST effort in order to more fully address the cybersecurity needs of the NSF facilities community. 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.

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

1.3 Webinar Series

Background. The Trusted CI webinar series[7] 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.

Progress this year. Trusted CI's Scott Russell presented a talk on legal insights regarding Cybersecurity Maturity Model Certification (CMMC) regulations in early October. It was a "one-off" presentation, not on the usual schedule, and was well received by our community. Also in October, Yuan Tien presented a talk on using natural language processing (NLP) to review privacy policies to help researchers when writing policy-compliant code. And in December, the Trustworthy Data Working Group hosted a panel discussion with Jim Basney, Sandra Gesing (PresQT), Bob Hanisch (NIST), and Rebecca Koskela (RDA-US). We spent the remaining weeks of 2020 scheduling the 2021 webinar season.

The 2021 webinar season began with a presentation on SciTokens. Project members presented their progress since presenting at the 2019 NSF Cybersecurity Summit. February's webinar was on the Cybersecurity in Application, Research and Education (CARE) Lab, presented by Aunshul Rege, a 2019 Trusted CI Fellow. We greatly enjoyed the opportunity to reconnect with Dr. Rege and to share her research on cybercrime. The March webinar was a summary of Purdue's Regulated Research Program (REED+) and its evolution from a controlled-unclassified information (CUI) environment, to an ecosystem, to a community. The presentation focused on lessons learned from implementing a compliance framework. Compliance presentations are often well attended and this one was no exception. The April webinar revisited the topic of Science DMZs with Douglas Jennewein and Chris Kurtz presenting a review of the installation at Arizona State University. May's webinar touched the topic of our 2021 Annual Challenge (Software Assurance) with Sagar Samtani's work identifying vulnerable GitHub repositories. Finally, the June webinar focused again on software assurance with Michelle Mazurek's presentation on secure development with a human-centered perspective.

Podcast. In May of this year we announced[8] a podcast version of our webinar. It is now available on Apple,[9] Google,[10] Overcast, Luminary, Pocketcasts, and many other podcatchers.

Metrics. Table 1 shows the number of webinar attendees and archive viewers in the reporting period.

[7] trustedci.org/webinars
[8] https://blog.trustedci.org/2021/05/trusted-ci-podcast.html
[9] https://podcasts.apple.com/us/podcast/trusted-ci-podcast/id1561008948
[10] https://podcasts.google.com/feed/aHR0cHM6Ly93d3cudHJ1c3RlZGNpLm9yZy90cnVzdGVkLWNpLXBvZD9mb3JtYXQ9cnNz

Table 1. Trusted CI Webinar attendance and archive viewing.

Month	Topic	Speaker(s)	Attended[11]	Watched Later[12]
Oct.	CMMC	Scott Russell	89	147
Oct.	Enforcing Policies	Yuan Tian	32	48
Dec.	Trustworthy Data panel	Basney & panelists	51	60
Jan.	SciTokens	Basney, Bockleman, & Weitzel	51	100
Feb.	CARE Lab	Aunshul Rege	52	59
Mar.	REED+ Ecosystem	Smith, Yang, & Ellis	87	88
Apr.	ASU's ScienceDMZ	Jennewein & Kurtz	53	122
May	ID'ing Vuln. Github Repos	Sagar Samtani	25	47
Jun.	Secure Dev. In Practice	Michelle Mazurek	10	9
Total			**450**	**680**

- Webinar registrants added to Announcements mailing list for the reporting period: 159
- Webinar registrants added to the Discuss mailing list for the reporting period: 146

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

1.4 Science Gateways Community Institute Partnership

Background. Trusted CI and the Science Gateways Community Institute[13] (SGCI) 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[14] within SGCI and works closely with that team (led by Claire Stirm at San Diego Supercomputer Center) to provide cybersecurity education and training for the gateways community.

Progress this year. The SGCI / Trusted CI partnership cybersecurity team attended the annual Gateways conference in October 2020. The cybersecurity team hosted a virtual table for Trusted CI to provide support for gateways in attendance. During the preparation and running of the conference, the Trusted CI team also offered security support and answered a few questions related to secure settings for video conferencing.

[11] Does not include Trusted CI staff and presenters.
[12] Viewed later on YouTube as of July 16, 2020.
[13] ACI-1547611
[14] https://sciencegateways.org/about/service-areas

The SGCI Focus Week held in December presented the opportunity for the cybersecurity team to provide pre-recorded content for SGCI Focus Week. This came in the form of a presentation of the regular Focus Week cybersecurity content and was uploaded to Youtube[15] where it is available publicly. This allows SGCI to reuse the content and is also a chance for the broader dissemination of the content beyond just the Focus Week attendees.

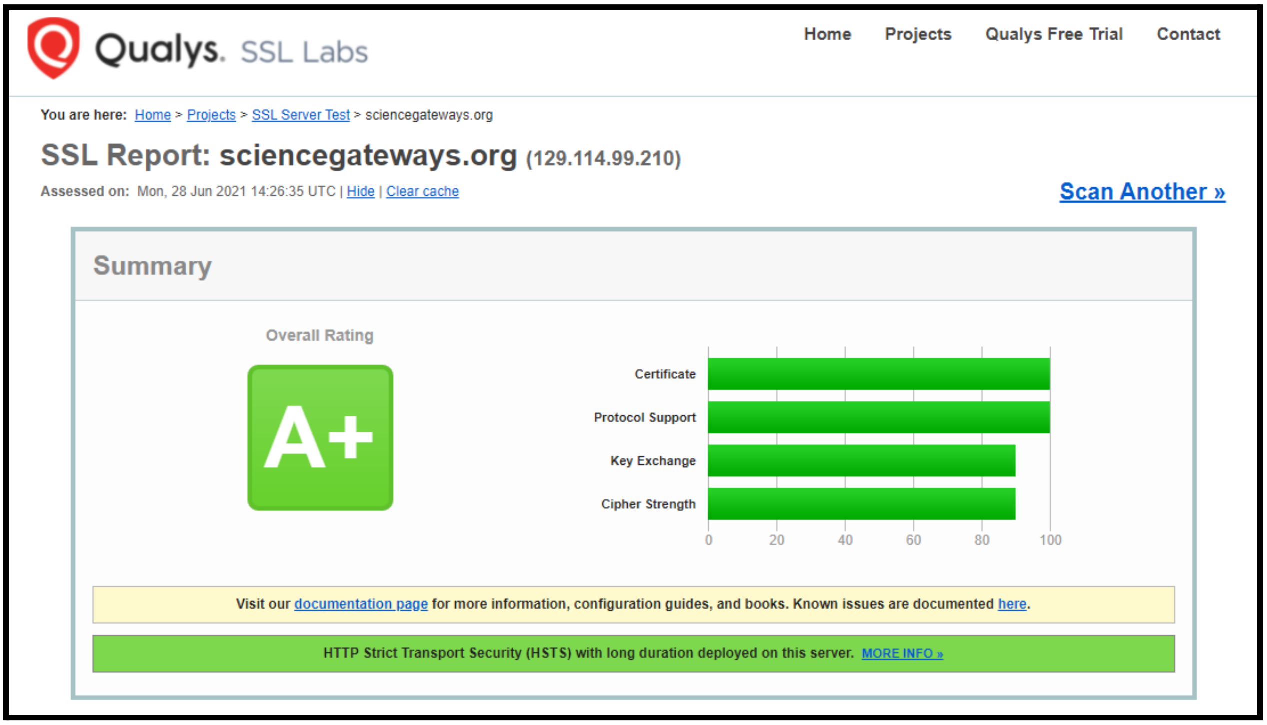
As a new way to utilize the resources from this partnership, three members of the cybersecurity team also worked on the Galaxy Project engagement, which is covered in section 3.5 of this document.

The cybersecurity team is also developing a mini-guide for science gateway projects that is based on the work of the Trusted CI Framework but tailored for the needs of the science gateway community. The team also presented “Cybersecurity for Gateways” at SGCI Jumpstart (Focus week) in the first week of March. The cybersecurity team also started two engagements with Geoweaver and Distant Reader in the months of February and March respectively. The cybersecurity team recently finished the Geoweaver engagement submitting the final security report to their PI. Completion of the Distant Reader engagement has been postponed at their request since Distant Reader’s allocation was coming to an end and might not have been extended past it’s due date.

The Trusted CI cybersecurity team also monitors the security status of sciencegateways.org website through ssl labs.org**.** As of the last scan (6/28/21), it received an A+ rating. At the request of SGCI, the team also performs backups of SGCI's cloud storage system to help mitigate the threats to cloud storage.

[15] https://www.youtube.com/watch?v=LKoFeciPOrA

Image 1. Qualys rating



You are here: Home > Projects > SSL Server Test > sciencegateways.org

SSL Report: sciencegateways.org (129.114.99.210)

Assessed on: Mon, 28 Jun 2021 14:26:35 UTC | Hide | Clear cache

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server.

Metrics. The team presented “Cybersecurity for Gateways” at SGCI Jumpstart (Focus week). Four of six people who responded to the survey said that the topic was relevant to their gateway and instructions were clear.

Plans for next year. The cybersecurity team will continue to work on the Miniguide to Science Gateway Cybersecurity, currently in review. The team will continue to work on the engagements as they are requested.

1.5 Trusted CI at PEARC

Background. Aside from the NSF Cybersecurity Summit, the Practice and Experience in Advanced Research Computing (PEARC) conference series is the highest profile event for Trusted CI. PEARC's impressive attendance (more than 800 people) gives members of Trusted CI many opportunities to network and share our work with NSF project team members. This year, PEARC21 (July 19-22, 2021) will be held as a virtual conference.

Progress this year. Members of Trusted CI submitted two presentation proposals and both were accepted:

- A workshop: The 5th Trusted CI workshop on Trustworthy Scientific Cyberinfrastructure[16]
  - The workshop provides an opportunity for sharing experiences, recommendations, and solutions for addressing cybersecurity challenges in research computing.
  - Jim Basney will be leading the three-hour workshop.
  - The call for presentations is currently open and will close on June 14th, 2021.
- A tutorial: Security Log Analysis: Real world hands-on methods and techniques to detect attacks
  - A half-day training ties together various log and data sources and provides a more rounded, coherent picture of a potential security event. It will also present log analysis as a life cycle (collection, event management, analysis, response) that becomes more efficient over time. Interactive demonstrations will cover both automated and manual analysis using multiple log sources, with examples from real security incidents.
  - Mark Krenz and Ishan Abhinit will be leading the tutorial.

Plans for next year. PEARC22 has not yet been announced. We will review the call for proposals and do our best to tailor our offering to the latest challenges the program wishes to address.

1.6 CI CoE Pilot

Background. Trusted CI and the CI CoE Pilot[17] 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
- Mature the engagement selection and planning process for the pilot
- Participate in meetings with the pilot's advisory committee

Progress this year. During the year the identity management working group met monthly a total of 11 times, with the exception of the month of December.

The working group discussed the following topics this year:

- July: REFEDS and International Federation (Tom Barton, Chris Whalen)
- August: ARF Engagement Post-mortem (Josh Drake, John Haverlack)
- September: Policy Lifecycles (Craig Jackson)
- October: Baseline Security Controls for IAM (Josh Drake)

[16] https://www.trustedci.org/pearc21-workshop
[17] https://cicoe-pilot.org/; #1842042

- November: Internet2 Community IAM Resources and the Incommon Trusted Access Platform (Jessica Fink, Erin Murtha, Paul Caskey)
- January: Review of Discussion Topics and Planning of 2021 Topics (IDM Working Group)
- February: Researcher Concerns for future IDM Standards and Common Identity Tracking and Sustainment Problems (IDM Working Group)
- March: Shibboleth Single Sign On Deployment (Paul Caskey)
- April: GAGE Engagement Post-Mortem (Josh Drake, Doug Ertz)
- May: Midpoint Middleware IAM Software (Slavek Lillyhammer)
- June: Grouper Access Management Software (Chad Redman)

Engagements. The working group concluded two engagements during the year, one with the Academic Research Fleet (ARF) from May-November 2020 and one with the GAGE facility from July to December 2020.

Final versions of engagement reports were provided to the Geodetic Facility for the Advancement of Geoscience (GAGE) and the Academic Research Fleet (ARF). The GAGE engagement post-mortem was conducted at the February Trusted CI All Hands meeting. A final GAGE engagement blog was posted and the GAGE engagement report was made available to the public on the Trusted CI blog and CI CoE website on March 30. The ARF blog post is on hold pending the results of ARF's proposal for funding to build the IdM system recommended in the engagement.

Due to operating under an NCE for 1H2021, no engagements were conducted, however an engagement with NOIR lab for 2H2021 was agreed and planned during Q2 2021.

The IdM working group began working with Seismological Facility for the Advancement of Geoscience (SAGE)/GAGE on a cloud platform design process as part of a larger engagement with all CI CoE Pilot working groups that will run for the first half of the year and produce a high-level cloud IdM service design.

Presentations and Community Involvement.

Josh Drake presented a session at Internet2's ACAMP conference in November 2021 focused on the scalability of commonly used IAM tools for major research facilities. Josh Drake joined Internet2's Community Architecture Committee for Trust and Identity (CACTI) in January 2021 for a two year term.

IdM working group personnel resumed the series of co-learning meetings, conducting deep dives into IAM topics and tools to create notes for cyberinfrastructure operators. The working group plans to publish a cookbook of IAM recipes at the end of 2021.

Metrics. Monthly working group participation:

- July: Twelve participants, five major facilities represented
- August: Nine participants, four major facilities represented
- September: Eight participants, four major facilities represented
- October: Seven participants, four major facilities represented
- November: Ten participants, five major facilities represented
- January: Seven participants, three major facilities represented
- February: Seven participants, four major facilities represented
- March: Eleven participants, six major facilities represented
- April: Ten participants, four major facilities represented
- May: Eight participants, four major facilities represented
- June: Six participants, three major facilities represented

Plans for next year. The CI CoE Pilot is expected to enter production as CI Compass. While CI Compass and Trusted CI will not have the co-funded staff that Trusted CI and the CI CoE Pilot did, the projects will continue to collaborate. The IdM working group is planning a 2H2021 engagement with NOIR Lab to assist in building out IAM infrastructure.

The notes from IdM co-learning meetings from 2020 and 2021 will be compiled into a “cookbook” of IAM tools or “recipes” to ease assimilation and implementation into major facilities cyberinfrastructure.

The IdM working group will continue to hold monthly meetings to discuss IAM topics for research facilities. The IdM working group is currently exploring opportunities to collaborate with the LFST and ResearchSOC for monthly discussion topics and presentations in 2H2021.

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. In Q4 2020, the project solicited feedback from the Trusted CI team regarding potential changes to the Community Survey questions. Additionally, the project developed a project plan for CY2021, which included onboarding a new team member, for increased project fault tolerance.

In Q1 2021, the Community Survey question set was updated to align with changes to the Trusted CI Framework, along with formatting and grammatical changes to improve readability.

The updated Community Survey was released to the community on March 29, with the response period ending on June 30. The Survey was distributed via the Trusted CI "Announce" listserv and the Trusted CI blog. The Survey was also informally announced during the February and March LFST calls. Finally, the Community Survey project successfully onboarded a second team member, Ishan Abhinit.

In Q2 2021, the project continued socializing the Community Survey, with monthly emails during April, May, and June, along with in-person reminders during the monthly LFST calls. Finally, the Community Survey response period closed on June 30, 2021.

Metrics. None.

Plans for next year. The Community Survey team will evaluate the results from the 2021 Survey, circulate preliminary findings within the Trusted CI Team, and publish a Community Survey Report in Q4 2021.

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 presentation activities to disseminate its work and to make NSF CI projects aware of its services.

Progress this year.

- Anurag Shankar presented the Trusted CI Framework at the IU Statewide IT conference[18] on Jan. 22 (Breakout Session 7).
- Bob Cowles presented talks on the Trusted CI Framework to the HEPiX Spring 2021 Conference and International Symposium on Grids & Clouds 2021 Security workshop in March.
- Von Welch conducted a presentation for the Canada Foundation for Innovation Major Science Initiatives Research Security workshop in March.[19]
- Craig Jackson and Susan Sons conducted a ReseachSOC webinar on the Trusted CI Framework.
- Von Welch provided a briefing on both Trusted CI and ResearchSOC to the JASON working group.
- Mark Krenz and Ishan Abhinit presented on Google Drive security at EDUCAUSE C&PPC. The presentation was well attended with 120 people in the audience. The content was based on the lessons learned from Trusted CI's use of Google Drive since 2014.

[18] https://statewideit.iu.edu/schedule/breakout/index.html
[19] https://www.innovation.ca/sites/default/files/pdf/MSI/trusted_ci_-_von_welch.pdf

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 its partners such as the OmniSOC and ResearchSOC to enable deployment of 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 advance their research and build a community capable of supporting each other in their TTP aspirations and activities. By engaging with cohort members we intend to learn about challenges they face when attempting to TTP and leverage that knowledge to develop methods and tools which can be used by others to successfully transition to practice. These methods and tools (TTP Plays) will be tested by cohort members and may be iterated over time. The products of these efforts will be published as they are completed on the Trusted CI website and catalogued in a TTP Playbook which describes how they may be used by others.

Progress this year. The TTP Cohort held nine additional regular monthly calls to discuss progress and challenges, as well as publishing an additional success story describing the path which motivated Dr. Pablo Moriano towards TTP. Version 1.0 of Trusted CI TTP Playbook was published on the Trusted CI website. The first two plays were developed in 2020 and published on the Trusted CI website.[20] These are the TTP TRL Assessment Tool and the TTP Canvas, which respectively are tools designed to help assess the maturity of the technology to identify next steps and to develop a plan to support the technology towards adoption.

Through discussions with the cohort regarding open source software topics we identified two topics which are promising candidates for playbook additions. These topics are open source licensing and operational cybersecurity data sources. We intend to explore further in the next year to determine what resources are already available to researchers as well as what new guidance should be incorporated into the playbook.

We did not achieve consensus with our proposed first TTP engagee regarding time commitment for an engagement as planned. Due to this, we refocused efforts and sought other engagement opportunities and identified Dr. Howie Huang as a strong candidate. We onboarded Dr. Huang into the cohort and in June we began an engagement with him to deploy a minimally viable prototype in collaboration with ResearchSOC and evaluate the prototype for potential operational use.

[20] https://www.trustedci.org/technology-transition-to-practice

Metrics.

- Onboarded Dr. Howie Huang to the TTP cohort and began the first TTP engagement in collaboration with both him and ResearchSOC.
- Published and announced v1.0 of the TTP Playbook, including descriptions of the first two TTP Plays.
- Held 9 additional cohort calls.
- Drafted proposal for 2021 NSF Cybersecurity Summit workshop

Plans for next year.

We will perform the following activities:

- Update descriptions of Trusted CI's TTP efforts on the Trusted CI website and publish a means by which researchers and other interested parties can contact Trusted CI about cybersecurity transition to practice.
- Identify one additional candidate for the TTP cohort and reach out to them to gauge interest.
- Continue to hold monthly TTP cohort discussions
- Conclude the first TTP Engagement to assist Howie Huang to deploy a prototype at ResearchSOC.
- Deliver the planned TTP Workshop at the NSF Cybersecurity Summit or if our workshop proposal is rejected identify an alternative venue.

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[21], blog page views, and unique website visits. Table 2 shows the statistics collected in the reporting period. The last row lists the statistics from the same period in the previous year.

Progress this year. There was a noticeable dip in Twitter impressions and website visits when comparing the same period in the previous year. This is likely due to the 2019 Summit being held in-person in October, whereas the 2020 Summit was virtual and held in September.

Our social media impact continues to maintain a steady progression in the current reporting period compared to the same period last year. One notable uptick was in blog page views in February 2021. After reviewing the posts, we attribute the increase to the announcement of the 2021 Fellows.

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

Metrics. Table 2 displays our social media impact during the project year.

Table 2. Social media impact during the reporting period

Date	Twitter Impressions	Blog Page Views	Website Visits
October	9.6K	7.4K	1.3K
November	9K	5.4K	.2K
December	4K	.4K	.6K
January	7K	2.8K	.7K
February	9.9K	7.3K	.6K
March	9.9K	11.2K	1.5K
April	7.3K	8.6K	1K
May	3.3K	8.3K	.6K
June	6.5K	7.7K	1.2K
Total Y2	**66.5K**	**59.1K**	**7.7K**
Previous year (for comparison)	130K	32K	9.2K

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 have transitioned office hours to a by-appointment format to accommodate community members' schedules.

Metrics. Since transitioning to office hours by appointment, we have received two inquiries that have been documented in consultations.

Plans for next year. Requesting office hours by appointment will remain an available option for working with Trusted CI.

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), 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, expedites risk management for open science projects and improves their cybersecurity. In 2019, Trusted CI personnel at Berkeley Lab expanded and evolved this document with the inclusion of details on data integrity issues, particularly those relating to bit flips.

Progress this year. In 2020, the same team expanded the OSCRP to better reflect the challenges that scientific researchers face when accessing and using data that is in some way sensitive and subject to restrictions on its access and use in order to protect confidentiality.

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 key issues and to enable more productive communication with each other.

In conjunction with Jim Basney, who led the 2020 Trusted CI Annual Challenge, we jointly presented on the 2020 Trustworthy Data Challenge and our 2019 data integrity report findings. In addition, updates to the 2019 data integrity report, based on findings from the 2020 Trustworthy Data Challenge, were completed in October 2020.

In the most recent quarter, an updated version of the data integrity report and confidentiality report were published, and a revised version of the OSCRP was published. All are available online:

- Reinhard Gentz and Sean Peisert, "An Examination and Survey of Random Bit Flips and Scientific Computing," Trusted CI Report, originally published December 2019, revised 2020. http://hdl.handle.net/2022/24910
- Sean Peisert, "An Examination and Survey of Data Confidentiality Issues and Solutions in Academic Research Computing," Trusted CI Report, 2020. https://escholarship.org/uc/item/7cz7m1ws
- Sean Peisert, Von Welch, Andrew Adams, Michael Dopheide, Susan Sons, RuthAnne Bevier, Rich LeDuc, Pascal Meunier, Stephen Schwab, Karen Stocks, Ilkay Altintas, James Cuff, Reagan Moore, and Warren Raquel, "Open Science Cyber Risk Profile," originally published February 2017, revised 2020. http://hdl.handle.net/2022/21259

The presenters of “Making Identity Assurance and Authentication Strength Work for Federated Infrastructures” at the International Symposium on Grids & Clouds[22] acknowledged use of the OSCRP in their presentation and paper. In particular, they made use of the section on asset classification.

As previously indicated, there are no specific plans to update the OSCRP in 2021, although we will continue minor maintenance updates. We expect to make more significant updates to the OSCRP in the future.

Metrics. The OSCRP has no milestones this year but we are tracking and responding to inquiries and tracking impact, such as the use of the OSCRP in the aforementioned paper.

Plans for next year. There are no specific plans to update the OSCRP in 2021/2022, although we will continue minor maintenance updates. We expect to make more significant updates to the OSCRP in the future, as needed and as new information is acquired, such as via the outputs of Annual Challenge exercises.

2.2 Situational Awareness / Cyberinfrastructure Vulnerabilities

Background. In collaboration with the ResearchSOC project[23] 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; and software developers OpenSSL, OpenSSH, and Globus. We also leverage 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 with those notifications. Trusted CI utilizes its existing email lists and encourages a dialog with our stakeholders for further discussions and feedback. All notices are archived and searchable from the Trusted CI email archives[24].

Progress this year. Between October 1, 2020 and June 30, 2021, 14 critical vulnerabilities were communicated to the community after evaluating a total of 32.

Metrics. The number of subscribers on the list increased from 159 as of September 30, 2020 to 168 as of June 30, 2021.

[22] https://indico4.twgrid.org/indico/event/14/session/15/contribution/4
[23] https://researchsoc.iu.edu/
[24] https://list.iu.edu/sympa/arc/cv-announce-l

Plans for next year. Operate as expected, evaluating vulnerabilities and communicating to the community as appropriate.

2.3 Publications

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

Progress this year. In March, the Trusted CI Framework team published the Framework Implementation Guide (FIG) for Research Infrastructure Operators Version 1.0. Section 2.6 includes additional details on this significant milestone event.

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 remote tutorials on Secure Programming and Automated Assessment Tools at Gateways'20 in October and at SuperComputing'20 in November. Both tutorials were a half-day long and included a hands-on segment on web security. The remote tutorial format allowed for substantially higher attendance than the normal in-person meetings.

Due to the pandemic, we did not deliver training in the first half of 2021. The effort made available by this pause has been redirected to other software assurance priorities (see section 2.5).

Plans for next year. In November, we will teach a full-day tutorial at SuperComputing'21. Our tutorial was accepted and at this time it is not clear if it will be an in-person or remote tutorial. We will deliver a series of training sessions, including a tutorial on web security and automated assessment tools, at the NSF Cybersecurity Summit.

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 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 lead in the development of an NSF cybersecurity ecosystem by training future and current software developers, which directly impacts trustworthy science.

Progress this year. Miller and Heymann produced several new video modules:

- FPVA step 1 (parts 1 and 2)
- FPVA Step 2
- FPVA Step 3
- Introduction to Fuzz Testing
- Classic Fuzz Testing
    - Section 1: Background
    - Section 2: Command Line Studies
    - Section 3: GUI-Based Studies
    - Sections 4 & 5: Other Studies
- Fuzz Testing with AFL
- Address Space Layout Randomization

All are available at https://research.cs.wisc.edu/mist/SoftwareSecurityCourse/.

The team developed new hands-on exercises on Fuzz testing. We updated our hands-on exercises to the latest available version of the different components of the software stack. Those exercises include Web attacks, exceptions, serialization, directory traversal, sql injection, command injection, XML injection, automated assessment tools, and thinking like an analyst and applying FPVA to find vulnerabilities.

Based on the materials developed under TrustedCI, Miller and Heymann taught their new *Introduction to Software Security* course (CS 542) to 100 students at the University of Wisconsin-Madison. Instruction was remote due to the COVID-19 pandemic. The remote format tends to alienate students so the team developed a variety of new interactive exercises for students to work in class in small groups and then discuss the results with the whole class. The team developed those exercises for all of the topics covered in CS 542.

Note that the topic of the 2021 Annual Challenge (see Section 2.12) is software assurance.

Metrics.

- Eleven video modules produced.
- Taught CS 542 to 100 students.

Plans for next year.

- Continue producing video modules for training.

- Make the hands-on exercise more easily accessible throughout our https://research.cs.wisc.edu/mist/SoftwareSecurityCourse/ web page.
- Continue teaching CS 542 (Introduction to Software Security) at the University of Wisconsin-Madison to 100 students.

2.6 Continuing Professional Education (CPEs)

Background. Continuing Professional Education (CPEs) are credits applied to the pursuit, or maintenance of, a professional certification. Trusted CI provides many educational opportunities that may fall under a cybersecurity certification programs' criteria for renewal. For example, Trusted CI currently provides documentation of attendance (e.g., a paper "certificate") at the NSF Cybersecurity Summit upon request. But, other trainings do not have corresponding documentation. This presents a missed opportunity to support the professional development of our community members.

In January 2021 we began a project to formalize the process for issuing and/requesting documentation. This project aligns with Trusted CI's mission of workforce development.

Badges are currently issued through Badgr[25], an open source badge issuing website. Badgr has features that allow recipients to share their badges on social media[26] (LinkedIn, Facebook, Twitter, etc.).

Progress this year. We began the project in January and issued our first badges to the previous years' Fellows, the 2020 Summit attendees, and started issuing badges to the webinar attendees in March. When the 2021 Fellows were announced we issued them badges as well.

The initial thrust of this project was completed in June. Moving forward we will issue badges as needed (monthly webinars, the 2021 Summit, and additional training/workshop opportunities).

[25] Trusted CI Badgr page: https://badgr.com/public/issuers/EhlDU1W_TnmOs8lD4O_j8A/badges

[26] https://support.badgr.com/en/knowledge/sharing-badges-on-social-media

Sample badges. Trusted CI reached out to Lauren Huber of Indiana University's IT Communication Office to design attractive badges that reflect Trusted CI's branding.

TRUSTED CI
Fellow 2021
TRUSTED CI
2021 Cybersecurity Summit Attendee
TRUSTED CI
Webinar Attendee 2021
TRUSTED CI
Training Attendee 2021
TRUSTED CI
Training Attendee 2021
TRUSTED CI
Training Attendee 2021

Metrics.

- 2020 Summit attendees - 35
- 2019, 2020, & 2021 Fellows - 20
- Webinar attendees (March 2021 - June 2021) - 91

Plans for next year. Badges are issued to community members who opt-in to receive a badge. Based on the positive feedback we've received from the community thus far, we will be continuing this program next year.

2.7 The Trusted CI Framework: An Architecture for Cybersecurity Program

Background. The Trusted CI Framework is a tool to help organizations establish and refine their cybersecurity programs. In response to an abundance of guidance focused narrowly on cybersecurity controls, Trusted CI set out to develop a new framework that would empower organizations to confront cybersecurity from a mission-oriented, programmatic, and full organizational life cycle perspective. Rather than rely solely on external guidance (which isn't tailored to the organization's mission and which may lack evidence of efficacy), the Trusted CI Framework recommends organizations take control of their cybersecurity the same way they would any other important business concern: by adopting a programmatic approach. This framework is designed to be understandable and usable by non-cybersecurity and cybersecurity experts alike.

Progress this year. In CY2021, the Framework Team tackled three significant initiatives

1) Completed content development of and published the Framework Implementation Guide (FIG) for Research Cyberinfrastructure Operators (RCOs);
2) Conducted a FIG early adoption engagement with NOIRlab;[27]
3) Launched a FIG socialization effort among the NSF community.

Published Framework Implementation Guide: We published version 1.0 of the Trusted CI Framework Implementation Guide (FIG) for Research Cyberinfrastructure Operators (RCOs)[28] on March 1, 2021. Developed by a team led by Craig Jackson, this guide is the culmination of many years of accumulated experience conducting cybersecurity research, training, assessments, consultations, and collaborating closely with the research community. Release of the first FIG represents a major step forward in advancing Trusted CI's mission to enable trustworthy science through cybersecurity guidance, templates, and tools, empowering those projects to focus on their science endeavors.[29]

This product was developed with significant advice and input from the Framework Advisory Board (FAB). The FAB is a body of 19 volunteers with diverse interests and roles in the education and research community that represent a cross section of the audience the FIG is designed to serve. The FAB provided substantial input, suggestions, questions, and critiques during the drafting of the FIG content. The list of FAB members and their organizational affiliations is below:

- 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.)

[27] https://noirlab.edu/public/about/
[28] *See* www.trustedci.org/framework for more information.
[29] A "Framework Implementation Guide" (FIG) is an audience-specific deep dive into how an organization would begin implementing the 16 Musts. FIGs provide detailed guidance and recommendations and are expected to be updated much more frequently than the Framework Core.

Conducted the NOIRLab FIG Early Adoption Engagement: In March 2021, the Framework Team began a special engagement with NOIRLab to assist them in adopting and aligning to the Framework, as well as to gather feedback / insights Trusted CI can use to revise the FIG and/or expand Framework-related offerings like tools and templates. The engagement featured an assessment of the organization's cybersecurity program as a whole and an evaluation of NOIRLab's alignment to the Trusted CI Framework as the foundation for their program. We used the PACT[30] methodology to structure the assessment and version 1.0 of the Trusted CI Framework Implementation Guide (FIG) for Research Cyberinfrastructure Operators (RCOs) as the standard. We concluded the assessment in June 2021 with the delivery of a Trusted CI Framework Assessment Report. The report leveraged the FIG as the primary resource for its recommendations and supporting rationales.

Launched a FIG Socialization Effort: In parallel with completing final activities to publish FIG v1.0 and conducting the NOIRLab early adoption engagement, the team made progress on socializing the Framework Implementation Guide. The purpose of this effort was to widely communicate the release of FIG v1.0 and encourage its use within and beyond the NSF community. We initiated this effort prior to the FIG's release and continued throughout the remainder of the PY2 reporting period. Socialization efforts included a combination of presentations, talks, email communications among Trusted CI Team members' professional and personal networks and blog posts. We attribute in part the more than 700 FIG downloads as of June 30, 2021 to the socialization efforts. Table 3 lists formal socialization presentations conducted during this reporting period.

Table 3. Framework socialization presentations.

Event	**Date**	**Presenter(s)**
Indiana University Statewide IT Conference	Jan 2021	Anurag Shankar
HEPiX[31] Spring 2021	Mar 2021	Bob Cowles
Canada Foundation for Innovation Major Science Initiatives Research Security workshop	Mar 2021	Von Welch

[30] The Principles-based Assessment for Cybersecurity Toolkit (PACT) is a collection of resources, templates, and tools supporting the standardized assessment of the toughest cybersecurity problems. This methodology was developed by the Center for Applied Cybersecurity Research in collaboration with the US Navy. For more information about PACT, *see* https://docs.google.com/document/d/1tegqFcTXqvwrPG2D_u58moIQUJhKGs_Pe2oGdXfHBpg/edit.

[31] HEPiX brings together worldwide Information Technology staff, including system administrators, system engineers, and managers from the High Energy Physics and Nuclear Physics laboratories and institutes, to foster a learning and sharing experience between sites facing scientific computing and data challenges(https://www.hepix.org/#section1).

International Symposium on Grids & Clouds (ISGC) 2021 Security workshop	Mar 2021	Bob Cowles
Research Security Operations Center (ReseachSOC) webinar	Mar 2021	Craig Jackson
Trusted CI Fellows Virtual Institute Presentation	May 2021	Craig Jackson
May WISE[32] Meeting	May 2021	Craig Jackson

In addition to these major activities, we prepared and submitted comments on the cybersecurity section of the December 2020 draft of the NSF Major Facilities Guide. Our recommendations included updating references from the old Guide to the Trusted CI Framework and FIG and adding language clarifying that “information systems” includes operational technology.

Metrics.

- Published FIG v1.0
- Completed the NOIRLab engagement Trusted CI Framework Assessment Report
- Achieved more than 700 FIG downloads and participated in seven formal socialization events.
- Provided Trusted CI comments on the NSF Major Facilities Guide

Plans for next year. The team will conduct a follow-on engagement with NOIRLab to help them formally adopt the Framework as the foundation of their cybersecurity program and implement high priority recommendations from the Trusted CI Assessment Report delivered in June 2021. Additionally, the team will leverage lessons from the NOIRLab early adoption experience to help prepare and implement efforts to scale Framework adoption across the NSF Major Facilities.

2.8 Broader Impacts

Background. Trusted CI is charged with addressing cybersecurity challenges affecting small projects, multi-institution collaborations, international collaborations and LFs. There are approximately 500 new NSF projects funded each year at $1 million or more, which indicates that they develop, use, or 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

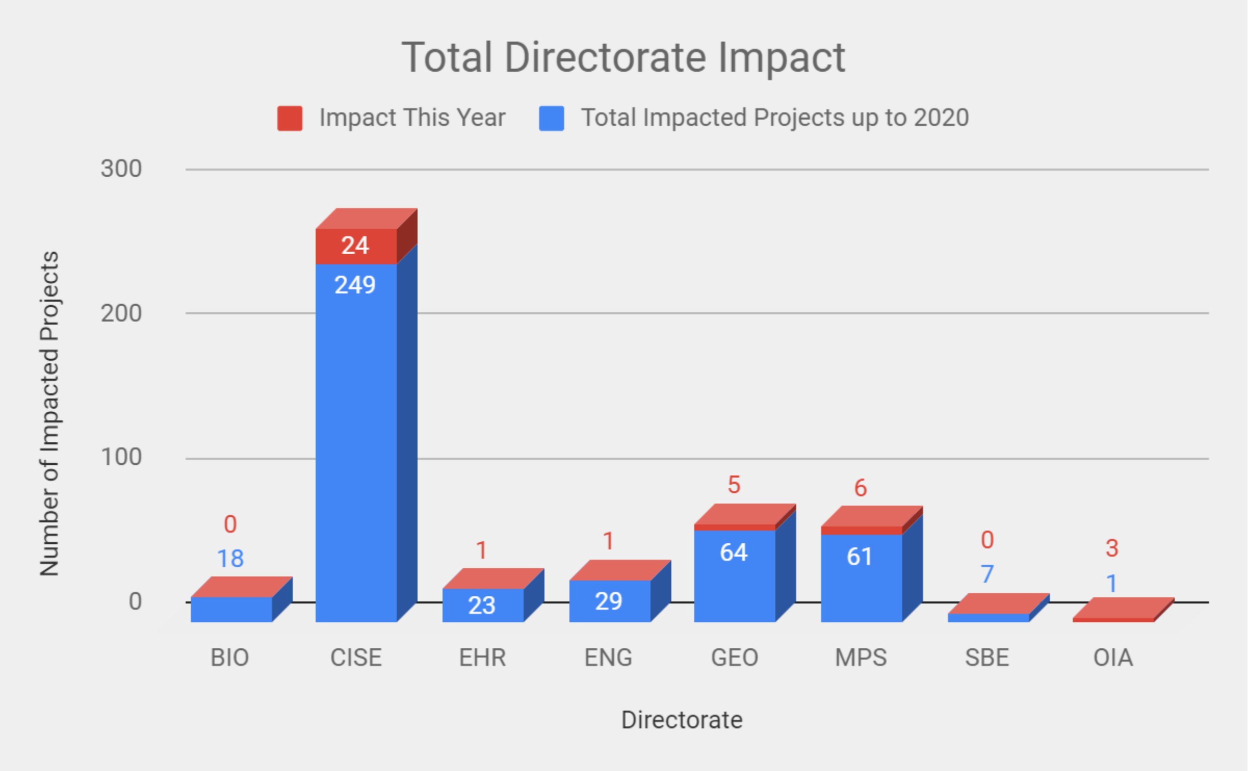
[32] WISE fosters a collaborative community of security experts and builds trust between IT infrastructures, i.e. all the various types of distributed computing, data, and network infrastructures in use today for the benefit of research, including cyberinfrastructures, e-infrastructures and research infrastructures (https://wise-community.org/about-wise/).

needs of a broader set of NSF projects (both small and large) and to provide demonstrated value to a significant percentage of NSF projects.

Progress this year. Metrics are continually updated with new statistics as Trusted CI events occur. This year, there were 473 individuals who attended Trusted CI webinars, and we impacted 41 NSF projects through these webinars. We also impacted 6 NSF projects through engagements in the first half of 2021.

Metrics. We continued to track project impact on a regular basis. The total number of NSF projects impacted by Trusted CI (over the lifetime of the project) is 492 projects. The total number of NSF projects impacted through each activity is: 162 through webinars, 334 through the summit, and 83 through engagements.

Image 2. Chart of total directorate impact



Plans for next year. We will continue to update our metrics regarding impact across NSF divisions.

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. The Call for Applications for the 2021 Fellows cohort opened during the 2020 Summit with applications due initially on Nov. 6 and extended to Nov. 20. The call was posted on the Trusted CI blog, via our announcements email list, social media and other community lists including the XSEDE Campus Champions, the CaRCC People Network, and CI Engineers.

Application requirements include:

- A description of the connection to the research community, including any NSF connections;
- A statement of interest in cybersecurity and what they hope to accomplish through their fellowship;
- A two-page biosketch;
- And a letter from their supervisor supporting their involvement and the time commitment to the program.

We received 25 applications for the 2021 Trusted CI Fellows cohort. These applications were reviewed by the Trusted CI leads, 2019 & 2020 Fellows, and Advisory Committee. We selected eight Fellows[33] from the applicant pool:

- Deb McCaffrey. Research Computing Facilitator at Michigan Medicine
- Amiya Maji, Senior Computational Scientist at Purdue University
- Dr. Elie Alhajjar, Research Scientist at the Army Cyber Institute
- Matthew Peterson, Senior Faculty Research Assistant at Oregon State University.
- Mauricio Tavares, Senior Security Engineer at FABRIC and FAB (FABRIC Across the Borders)
- Richard Wagner, Systems Integration Engineer at University of California, San Diego
- Shuyuan Mary Ho, Associated Professor at Florida State University
- Michael Kyle, Scientific Applications Consultant at University of Delaware

The Trusted CI Virtual Institute commenced its weekly sessions on March 29 with introductions, logistics, and an overview of Trusted CI.

[33] Reduced participant travel expenses due to the pandemic allowed us to expand the cohort.

Metrics. Twenty-five applications were received.

Plans for next year. This year's future featured speaker is Subha Sivagnanam, talking on Open Science Chain and the Blockchain which the Fellows have requested. The 2021 Fellows will attend PEARC & NSF Summit which will be held virtual. The Call for Applications for the 2022 Fellows cohort will be announced during the 2021 NSF Summit in October.

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 2021, 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, General Data Protection Regulation (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. In Q3 2020, the project onboarded one new CACR-Maurer Student Affiliate for Fall 2020, selected for their research topic "the impact of European privacy law on intellectual property rights," and began drafting the preliminary draft of the research memo. In Q4 2020, the project finalized the research memo from the CACR-Maurer Student Affiliate for Fall 2020, including student affiliate research presentations at a CACR Privacy and Security Lunch Talk. Additionally, the project drafted a project plan for CY2021.

In Q1 2021, the project onboarded two new Student Affiliates for the semester. The two student affiliates selected the following deep dive topics into GDPR compliance for research and higher education facilities, specifically: 1) understanding applications of the "legitimate use" lawful purpose for research and higher education facilities; and 2) understanding when and how GDPR governed data can be subject to U.S. civil discovery. The student affiliates submitted outlines and first drafts of their research memoranda in February and March 2021, respectively. In Q2 2021, the student affiliates finalized their revisions to the draft memoranda.

Metrics. None.

Plans for next year. The project will present at the Trusted CI Webinar Series in Q3 2021, as well as continue its collaborations with the CACR-Maurer Student Affiliates program.

2.11 Quilt Collaboration

Background. A new activity in 2020, the goal of this project is to leverage a collaboration with the Quilt[34] 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 was 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. Due to pandemic travel restrictions, the plan evolved to have a virtual workshop wherein the interested Quilt members would form teams with campus research computing, security, and networking professionals and participate in a virtual workshop. Unfortunately, their ability to participate in this workshop decreased as the pandemic wore on, but through our discussions, we learned that more groundwork is needed to build connections between the regionals and their campus research computing and security groups.

Progress this year. The pandemic continued to hamper the ability of the regional networks to participate in the collaboration. As a consequence, we decided to delay the workshop and continue discussions with the regionals until the distraction from the pandemic eases. Through our discussions, it became apparent that regional networks in general do not have strong connections with their member researchers and research-supporting IT staff, so this delay provides an opportunity to build additional groundwork needed.

During the 2nd half of 2021, we are engaging with the University of Arkansas on their EPSCoR award. A significant component of that engagement will be the facilitation of their multi-institutional ScienceDMZ, a topic of broad interest to the Quilt's constituency and the NSF community. Hence we are partnering with the NSF Engagement and Performance Operations Center (EPOC)[35] in our engagement with the University of Arkansas and will turn the results of that engagement into training products that we disseminate through the Quilt to the Regionals.

During these discussions, Trusted CI participated in the Winter 2021 Quilt meeting to discuss security of research cyberinfrastructure.

With the departure of co-PI Brunson from Trusted CI, Mark Krenz is now leading this effort.

Plans for next year. Trusted CI will complete the engagement with University of Arkansas and work with the Quilt to develop training to deliver at their Winter Member meeting.

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

[35] Award #1826994

2.12 Annual Challenge

Background. In 2021, Trusted CI is embarking on an Annual Challenge that seeks to broadly improve the robustness of software used in scientific computing with respect to security. It is doing this by spending the first half of 2021 engaging with developers of scientific software to understand the range of software development practices and evaluate potential deficiencies in practice or code implementation that lead to vulnerabilities. In the second half of 2021, we will leverage our insights to develop a guide specifically aimed at the scientific software community that covers software assurance in a way most appropriate to that community, rather than existing guides that have different foci.

Progress this year. We completed the work of the Trustworthy Data Working Group[36], a collaborative effort of Trusted CI, the four NSF Big Data Innovation Hubs[37], the NSF CI CoE Pilot[38], the Ostrom Workshop on Data Management and Information Governance[39], the NSF Engagement and Performance Operations Center[40] (EPOC), the Indiana Geological and Water Survey[41], the Open Storage Network[42], and other interested community members. The goal of the working group was to understand scientific data security concerns and provide guidance on ensuring the trustworthiness of data. In October 2020, we presented our work to the Big Data Hubs Data Sharing and Cyberinfrastructure Working Group and at the SGCI Webinar. In December 2020, we held a Trustworthy Data Panel for the Trusted CI Webinar and we published final versions of our survey[43] and guidance[44] reports.

In January, the Annual Challenge team evaluated and documented gaps in existing software assurance frameworks, developed and documented a process for engaging software teams, and developed a form for gathering input useful for producing a guide based on the results. In February, the team compiled a list of software teams to interview/examine that spanned numerous NSF directorates. In March, the team conducted its initial interview and compiled a written analysis from that interview. It also posted a blog[45] introducing the goals of the annual challenge.

Since then, Trusted CI has interviewed six teams developing software for scientific computing and cyberinfrastructure. It has collected its findings and is in the process of summarizing these

[36] https://trustedci.org/trustworthy-data
[37] https://www.bigdatahubs.org
[38] https://cicoe-pilot.org
[39] https://ostromworkshop.indiana.edu/research/data-management
[40] https://epoc.global
[41] https://igws.indiana.edu
[42] https://www.openstoragenetwork.org
[43] https://doi.org/10.5281/zenodo.3906865
[44] https://doi.org/10.5281/zenodo.4056241
[45] https://blog.trustedci.org/2021/03/announcing-2021-trusted-ci-annual.html

at a high level for a public blog post. It has also developed the goals of and outline of the guide planned for development in the second half of the calendar year.

Metrics. Expected tasks and milestones have been completed. Six software projects enthusiastically agreed to meet with us and our interviews span four NSF directorates: BIO, CISE, GEO, and MPS.

Plans for next year. In the next quarter, the 2021 Annual Challenge team will begin development of a written software assurance guide. A presentation proposal will be submitted to facilitate presentation of preliminary elements of findings and guidance at the NSF Cybersecurity Summit. Planning will also commence in for the 2022 Annual Challenge on Cyber-Physical System Security, and work on that Challenge will commence in full in January 2022.

2.13 National Leadership in Research Cybersecurity

Background. With an increasing national emphasis on research security,[46] cybersecurity for research is similarly receiving national attention. Trusted CI is taking a role in this national conversation to ensure the cybersecurity challenges of NSF science are understood and hence efforts at the national level result in outcomes that strengthen NSF science integrity, trustworthiness, and reproducibility, while minimizing negative impacts on its productivity.

Progress this year. Trusted CI PI Von Welch is engaged with an advisory group formed by EDUCAUSE and the REN-ISAC, which works closely with the Council on Governmental Relations (COGR) and legislative liaisons at various universities to educate national leaders on the range of cybersecurity research challenges faced by higher education and the NSF community[47]. Organized by that group, Von Welch gave a presentation at the Council on Governmental Relations (COGR) annual meeting emphasizing how to balance DoD security requirements (CMMC) with NSF science needs.[48] Additionally, as described in Section 1.8, Von Welch was an invited speaker at the Canadian Foundation for Innovation Major Science Initiatives workshop on cybersecurity, and an invited speaker by the JASON working group at their summer session exploring cybersecurity for NSF Major facilities.

Plans for next year. We will continue to work with the EDUCAUSE advisory group and look for opportunities to engage with national leadership and groups such as JASON on this issue.

[46] E.g. https://www.nsf.gov/news/news_summ.jsp?cntn_id=299700

[47] E.g. https://er.educause.edu/blogs/2020/12/educause-raises-concerns-about-dod-cmmc-800-171-assessment-rule

[48]

3 One-on-One Collaborations: Engagements

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

3.1 Engagement Applications

Background. Trusted CI directly supports individual NSF cyberinfrastructure projects and large facilities through collaborative engagements that address specific project needs. Trusted CI engagement activities include (but are not limited to) security reviews, security architecture design, IdM, and software assurance. Twice per year, we solicit 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. We opened and publicized a call for applications and selected engagements to be executed in the first half of 2021 and have completed those engagements. We selected engagements for the second half of the calendar year, assigned engagement leads and supporting team members as well as allocated effort for the second half of the calendar year.

Metrics. We opened and publicized a call for applications to be executed in the second half of 2021. We received 4 applications and accepted all 4.

Plans for next year. We will open and publicize a call for applications in August and select engagements to be executed in the first half of 2022.

3.2 Engagement Success Stories

Background. Trusted CI has been building a reservoir of successful engagements for nearly a decade. Many accomplishments are detailed on the Trusted CI blog[49] and on the Cybersecurity TTP page.[50] In 2020, Trusted CI began reaching out to its community, gathering the impacts of its engagements, and summarizing them into Trusted CI Success Stories. Seven have been published on the Trusted CI Success Stories page.[51]

Progress this year. Trusted CI completed six success stories on the AoT, Gemini, OpenXDMoD, Pegasus, TransPAC, and Wildbook[52] engagements.

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

[50] https://www.trustedci.org/technology-transition-to-practice

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

[52] https://static1.squarespace.com/static/5047a5a6e4b0dcecada15549/t/6021937dc40b1b54226dfacd/1612813182666/TrustedCI-success-story-Wildbook.pdf

Metrics. Trusted CI plans to post at least one success story per quarter as engagements are recommended by engagement leads.

Plans for next year. A success story on the USARF engagement is in review with ARF and will be posted in the first quarter of next year (July 2021).

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.

- Contacted by researcher Luanzheng Guo regarding his search for data products to use in his research, Trusted CI spoke with him to understand the types of cybersecurity research he was seeking to do and identify potential partner organizations in the NSF community which may have relevant data sets available.
- The Minnesota Supercomputing Institute is in the process of bringing up a HIPAA-compliant HPC resource for campus. Trusted CI reviewed MSI’s approach and provided guidance on how best to address certain aspects of vendor agreements (particularly for storage vendors) and the compliance and documentation for common software applications.
- Von Welch consulted with Jeff Pummill at University of Arkansas on their migration of their HPC infrastructure to their Science DMZ. This contributed to their subsequently submitting an engagement application.
- Sean Peisert consulted with UC Merced to conduct a peer review of their network redesign.
- Mark Krenz provided Google drive expertise to the CaRCC group (via Dana Brunson). This was based on Trusted CI's own experience using it and providing some solutions for backups, permission auditing, and Trusted CI's offboarding process

3.4 FABRIC

Background. FABRIC: Adaptive Programmable Research Infrastructure for Computer Science and Science Applications, funded under NSF grants 1935966 and 2029261, is a national scale testbed that connects to prior existing testbeds, such as PAWR, as well as the real Internet. FABRIC aims to expand its outreach, enabling new science applications, using a diverse array of networks, integrating machine learning, and preparing the next generation of computer science researchers. The FABRIC project began in 2019 and reached out to Trusted CI for an engagement during this early phase of development. The engagement goals were focused on reviewing FABRIC's software development process, the trust boundaries in the FABRIC system, and the FABRIC security and monitoring architecture.

Progress this year. The five-month engagement began in February 2021 and completed in June 2021. In that time the FABRIC and Trusted CI teams worked together to review FABRIC’s project documentation, which included a deep analysis of the security architecture. We moved on to completing an asset inventory and risk assessment, covering over 70 project assets, identifying attack surfaces and potential threats, and documenting current and planned security controls. Lastly, we documented engagement findings in an internal report shared with FABRIC project leadership.

FABRIC also assisted with the Trusted CI 2021 Annual Challenge (Software Assurance) by participating in an interview with members of the software assurance team. The results of that interview will provide input to Trusted CI's forthcoming guide on software assurance for NSF projects.

Plans for next year. Post-engagement plans include publicly releasing a redacted engagement report and organizing a testbed facility security workshop at the 2021 NSF Cybersecurity Summit.

3.5 Open OnDemand

Background. Open OnDemand[53] is funded by NSF Office of Advanced Cyberinfrastructure (OAC) and is an open-source high performance computing (HPC) portal based on the Ohio Supercomputer Center’s[54] original OnDemand portal. The goal of Open OnDemand is to provide an easy way for system administrators to provide web access to their HPC resources. Open OnDemand is now facing increased community adoption. As a result, it is becoming a critical production service for many HPC centers and clients. By improving the overall security of the project, we will ensure that it continues to be a trusted and reliable platform for the hundreds of centers and tens of thousands of clients that regularly utilize it.

Open OnDemand has engaged with Trusted CI to support their efforts to further develop the project’s ability to produce secure software. Trusted CI previously conducted an in-depth vulnerability assessment applying the First Principles Vulnerability Assessment (FPVA) methodology to Open OnDemand software. The results of this prior assessment will help to inform the activities of this engagement. During the course of the prior FPVA assessment, Trusted CI staff worked directly to test Open OnDemand’s software to identify vulnerabilities with support from the Open OnDemand team. Trusted CI will now work with Open OnDemand

[53] https://openondemand.org/
[54] https://www.osc.edu/

to improve the project’s ability to maintain the security of their software as changes are made and to identify and mitigate future vulnerabilities.

Progress this year. In the first half of 2021, we began and completed an engagement with the Open OnDemand team. The engagement included coaching Open OnDemand regarding utilizing the FPVA methodology as well as creating checklists which Open OnDemand developers can use at critical stages of code development and release. In addition, we began analysis of available dependency checking and static analysis tools and recommended tools for Open OnDemand’s use. Lastly, we began coaching the Open OnDemand team regarding the creation of critical architecture diagrams which will enable them to conduct internal first principles vulnerability assessments in the future.

Metrics. We successfully completed the engagement.

Plans for next year. We will publicly release a redacted version of the engagement report.

3.6 Partnership to Advance Throughput Computing

Background. The Partnership to Advance Throughput and Computing (PATh) is a project funded by NSF’s OAC Campus Cyberinfrastructure (CC*) program and brings together the Center for High Throughput Computing and the Open Science Grid (OSG) in order to advance the nation’s campuses and science communities through the use of distributed High Throughput Computing. The PATh project offers technologies and services that enable researchers to access through a single interface, and, from the comfort of their “home directory”, computing capacity offered by a global and diverse collection of resources.

The engagement is focusing on evaluation and review of PATh’s and OSG’s current security plan, revising and removing outdated policies, and creating new policies to address gaps in coverage. This work is being guided by Trusted CI’s Framework and the FIG.

Progress this year. The Trusted CI and PATh teams had a pre-engagement meeting to discuss the plan and scope of the engagement and review their security plan as part of an NSF award requirement. A Security Program Evaluation was completed and the teams worked on becoming familiar with the current PATh/OSG policies, the Trusted CI Framework, and FIG. Current policies were reviewed, then mapped to the Framework Must’s to guide the direction and prioritization of the security plan rewrite. PATh/OSG conducted interviews to identify critical assets and then used this information to perform a baseline control set crosswalk. These exercises sparked discussions leading to additional gap identification, mitigation strategies, risk assessment and acceptance, and prioritization of these tasks.

Plans for next year. With approval from PATh, we will release a final report which will outline the engagement activities, identified gaps, plans to mitigate, and recommendations from Trusted CI.

3.7 Michigan State University

Background. Michigan State University (MSU) experienced a ransomware attack in May 2020.[55] While many organizations attempt to keep the public from finding out about cyberattacks for fear of loss of reputation or follow-up attacks, MSU has decided to make elements of its attack public in the interests of transparency, to encourage disclosure of similar types of attacks, and perhaps more importantly, to educate the open-science community about the threat of ransomware and other destructive types of cyberattacks. The overarching goal is to raise awareness about rising cybersecurity threats to higher education in hopes of driving safe cyberinfrastructure practices across university communities.

To achieve this, the CIO's office at MSU will engage with Trusted CI in a collaborative review and analysis of the ransomware attack suffered by MSU last year. The culmination of the engagement will be a report focusing on lessons learned during the analysis; these lessons learned would then be disseminated to the research community. We expect the published report to be a clear guide for researchers and their colleagues who are security professionals to help identify, manage, and mitigate the risk of ransomware and other types of attacks.

Progress this year. We interviewed personnel from MSU regarding their role during the incident and its response as well as their observations. Moreover, we presented our process, observations and recommendations to EDUCAUSE's Cybersecurity and Privacy Professionals Conference. Finally, we drafted a report focusing on the 'lessons learned', which is currently being reviewed by the MSU ISO for publication approval.

Metrics. The final deliverable of this engagement -- the lessons learned report alluded to above -- will offer utility to the scientific community in bolstering its security posture. Moreover, a secondary metric of success would be realized if this report (and process) encouraged other academic-based organizations that have experienced a breach to share and publish their lessons learned.

Plans for next year. Upon approval from MSU, we will disseminate the report through Trusted CI's blog, at a minimum.

[55] https://msutoday.msu.edu/news/2020/msu-provides-update-on-it-based-intrusion

4 Engagement Evaluations

Since August 2016 we have routinely followed up with prior engagements to assess long-term impact and our own engagement processes. We have received 39 responses to our Engagement Evaluation Questionnaire[56] to date, including 6 responses in PY2. 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 33 of 39 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 five responses were 4 out of 5 ("Very Likely") on Question 7.

However, not every response indicates maximum positive impact. Several respondents identified barriers to the engagement having more positive impact, mostly commonly selecting "Other priorities diverted attention from cybersecurity" and "Insufficient staff/budget/resources to make recommended changes." The 2021 responses indicate that these barriers are more prevalent than they have historically been and that the COVID-19 pandemic posed an unexpected barrier for our engagees.

The 39 responses include 29 first time evaluations, 6 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 39 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.

22 of 36 responses were 5. All 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 37 responses indicated any negative impact, each with a rating of 1 ("low").

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

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 (25)
- Increased cybersecurity knowledge among staff and personnel (24)
- Understanding cybersecurity risks to the science mission (23)
- Communication of risks to decision-makers and stakeholders (22)
- Improved governance / policy / risk acceptance structure (21)

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

- 9 responses indicated "Improved governance / policy / risk acceptance structure."
- 6 responses selected "More security or efficient identity and access management."
- 6 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."
- 14 responses selected "Other priorities diverted attention from cybersecurity."
- 12 responses selected "Insufficient staff/budget/resources to make recommended changes."
- 8 responses selected "Insufficient project or facility resources applied to engagement."
- 6 responses selected "inadequate buy-in from decision makers or stakeholders"

Q6. Which one of the barriers was most significant?

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

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

33 of 37 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. 35 of 37 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 engagement along 4 variables. The responses generally indicate that engagees believe they receive superior service from Trusted CI.

- **Usefulness**. 4 ratings of "much better"; 12 of "somewhat better"; 6 of "about the same".
- **Quality of communication**. 7 ratings of "much better"; 7 of "somewhat better"; 5 of "about the same".
- **Quality of deliverables**. 4 ratings of "much better"; 13 of "somewhat better"; 5 of "about the same".
- **Positive impact on security**. 4 ratings of "much better"; 9 of "somewhat better"; 8 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.

24 of 32 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?

26 of the 30 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?

22 of the 28 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.

3 thumbs up, Trusted CI

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
- Budgeting/overseeing spending
- Establishing program templates, policies, and procedures
- Reporting

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

Progress this year. In response to the 2020 AC meeting (see 5.2), we held a Trusted CI leadership retreat focused on the program's strategic objectives. We completed the effort allocation for 2021, ensuring appropriate resource alignment to program activities.

We delivered the quarterly report reflecting progress for Q42020 and Q12021 as well as the 2021 project execution plan. We began the process of documenting key performance indicators (KPIs) in support of our strategic goals[57] and presented those to the Advisory Committee (see section 5.2).

Metrics. We held two quarterly Advisory Committee meetings (see section 5.2). We delivered our quarterly reports and project execution plan as scheduled.

Plans for next year. We will continue our regular leadership and all team recurring meetings. We will finalize our program KPIs based on Advisory Committee feedback and adjust our activities and effort allocations accordingly. We will then begin the process of aligning our KPIs to the 30- and 48-month review questions and documenting our accomplishments in preparation for a March 2022 review.

5.2 Advisory Committee Changes and Meeting

Background. The Trusted CI Advisory Committee serves to provide Trusted CI with strategic guidance. White it has historically convened for an in-person meeting each year co-scheduled with the SuperComputing conference, we have shifted to quarterly virtual meetings due to the pandemic. 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, Chief Information Officer at Alabama A&M
- Ewa Deelman, Research Professor of Computer Science and Principal Scientist at USC Information Sciences Institute, PI 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 and Chief Information Officer at Michigan State University

Their bios can be found on the Trusted CI website[58].

Progress this year. We held our annual Trusted CI AC meeting Nov. 2-3, 2020. The meeting was held virtually. During the sessions, we solicited AC input on key program activities and established a list of takeaways for follow up. The pandemic requires we continue to meet

[57] https://scholarworks.iu.edu/dspace/handle/2022/22178
[58] https://trustedci.org/advisory-committee

virtually for the foreseeable future. As a result, we elected to shift to a quarterly meeting schedule (instead of annual) to minimize the need for context-setting at the start of each session.

The pandemic has necessitated that we meet with the Advisory Committee virtually instead of face-to-face. As a result, during our November 2020 meeting, we elected to meet quarterly in 2021 to enable more productive and ongoing discussions about program strategy. We held our first quarterly meeting with the Advisory Committee on March 10 with a focus on discussing and revising our draft KPIs. We also presented updates on takeaways from the November 2020 meeting. We held our second quarterly meeting on June 9 and presented updated KPIs along with a more in-depth discussion of why we feel establishing these KPIs and more clearly defining the communities we serve is valuable.

Metrics. The meetings were held successfully (though virtually) and resulted in a series of actionable takeaways for program improvement.

Plans for next year. We will deliver final KPIs to the AC for review and establish a plan for implementing the KPIs into our program activities in 2022.

5.3 Trusted CI All Hands Meeting

Background. Each year, we hold the Trusted CI all hands meeting, 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. Due to the pandemic, we decided to indefinitely postpone the 2021 All Hands Meeting (which would usually occur in March). We will reconsider holding the event when travel is deemed safe again.

Plans for next year. We will continue to monitor the implications of the pandemic and consider if holding an in-person event is safe.

5.4 Project Changes from the Project Execution Plan

Background. Each year, we deliver a project execution plan (PEP) including a summary of each major program activity, our expenditures plan, the details of our program governance plan, and a change management plan. As part of our change management plan, we communicate small changes to the project via our quarterly reports.

Progress this year. We created and delivered the 2021 PEP which includes CY2021 project plans for all key program activities.

Plans for next year. We will deliver an updated PEP for 2022 which reflects the changes resulting from the newly defined KPIs and project goals.

5.5 Personnel changes

The following personnel changes occurred during the reporting period:

- Indiana University (CACR) - Anurag Shankar and Will Drake have stepped away from Trusted CI.
- Internet2 - Dana Brunson discontinued her role on the project and Internet2 is no longer affiliated with Trusted CI.
- University of Illinois (NCSA) - no changes
- University of Wisconsin - Ian Ruh stopped working for Trusted CI and Ritvik Bhawnani, an undergraduate student, joined the University of Wisconsin team.
- Pittsburgh Supercomputing Center - no changes
- Lawrence Berkeley National Laboratory - Reinhard Gentz has temporarily reduced effort to minimal. Jason R. Lee from LBNL's NERSC division was added to the Berkeley Lab's Trusted CI team to assist with the 2021 Annual Challenge on Software Assurance and is expected to continue in 2022.

5.6 ResearchSOC Collaboration

Background. Trusted CI PI Von Welch also directs the ResearchSOC project[59], 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)
- Alignment of ResearchSOC security and operational metrics with the Trusted CI Framework (see Section 2.6)
- Outreach: ResearchSOC presents to the LFST (see Section 1.2) and at Trusted CI-hosted events (PEARC and the NSF Cybersecurity Summit).

Progress this year. We began a series of quarterly meetings with Trusted CI and ResearchSOC leadership to discuss additional opportunities for collaboration and cross-promotion of events. Susan Sons and Craig Jackson presented the Trusted CI Framework on a ResearchSOC webinar.

Metrics. Seven points of collaboration.

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

Plans for next year. We will continue our quarterly meeting series with the next session scheduled for July 23.

5.7 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, where possible, to Trusted CI assets; and staying abreast of current vulnerabilities and threats.

Progress this year. The security team completed policies for GDrive folder labeling tags, onboarding and offboarding, and in vanguard of the release of the Trusted CI Framework, updated our Master Information Policies and Procedures document to highlight the Framework Musts, while additionally reviewing, updating and publishing every policy document identified in our security program. Additionally, the team set up and put into production a ticketing system (RT) used to track security maintenance and incident tasks.

The GDrive backup, ASAPS, and usage policy documents were also developed, and several tests were performed to vet the restoration procedure. Regular maintenance performed by the team includes: the onboarding of two new staffers, the offboarding of 3, and the execution of tabletop exercises focusing on phishing and ransomware attacks.

Metrics. The team completed the majority of the tasks it laid out in their 1-2Q2021 project plan; 'testing backup restores,' 'updating the Trusted CI website to include the new DOIs for our published security program,' and 'activating and publishing our GDrive policy' remain unfinished.

Plans for next year. Continue to address tasks within the 2021 project plan, and if needed, perform incident response.

6 International Travel and Impact

During PY2, the Trusted CI team undertook no international travel under Trusted CI funding.

7 Metrics

Table 4. Trusted CI activity goals and achieved metrics.

Activity	Measurement Technique	Goals	Achieved
Engagements with NSF projects.	Direct measurement of the number of engagements.	4-6/year depending on complexity.	On track. Seven engagements completed in the end of 2020 (Galaxy, Open Storage Network, SCIMMA, SOCCOM, UC Berkeley, XSEDE Metric Service) and Five engagements completed in 2021 (FABRIC, NOIRLab, Open OnDemand, PATH, MSU)
	Post-engagement survey.	High ratings of engagement utility.	On track. See Section 4 for new results.
	Consultations (new)	None.	4 (see Section 3.3)
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 in 2021 will have details published in Q4 2021 in a report, and will include information regarding NSF projects that are using the Trusted CI framework or guide.
Cyberinfrastructure Vulnerabilities / *Situational Awareness*	Direct measurement of number of individuals and NSF projects receiving announcements.	90%+ of Large Facilities receiving announcements by end of YR1. Aim to increase linearly.	Currently 13 out of 20 Large Facilities Programs represented on our list (65%).

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

Activity	Measurement Technique	Goals	Achieved
Training	Direct measurement of attendance.	50 members of NSF community per year attending.	245 attendees from the NSF community attended training provided by Trusted CI staff. 150 Attendees at the 2020 NSF Cybersecurity Summit 20 Attendees at Secure Programming and Automated Assessment Tools at Gateways 2020 75 Attendees at Secure Programming and Automated Assessment Tools at Supercomputing'20
	Survey of attendees.	100% rating training as valuable.	Of 22 people surveyed for Summit training day, 91% said they would participate in training at future summits. 100% of the responses found the training useful.
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 142 NSF-funded projects including 16 large facilities.
	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 received responses from 26 attendees. To the question "How would you rate your overall experience with the 2020 summit?" 10 respondents answered that the quality of the summit was Excellent (highest rating) and 11 answered Good (2nd highest).
	Number of groups using online training materials	Linear progression each year.	Nothing to report yet.

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

Activity	Measurement Technique	Goals	Achieved
Outreach / Community Impact	Presentations at Project/PI Meetings	4-6 per year	On track. Presentations IU Statewide IT conference, Cybersecurity for Leadership bootcamp at Look Listen, HEPiX Spring 2021 Conference and International Symposium, presentation at Canada Foundation for Innovation Major Science Initiatives Research Security Workshop, and a ResearchSoc webinar
	Mentions in NSF Solicitations	Goal is all solicitations with a requirement for a cybersecurity program to mention us as a resource.	Two: NSF 21-037, 21-512. Plus pointer to Trusted CI on Large Facility Office website.
	Webinar attendance and views of archives (new)	Continued growth	Attendance: 450 Archive views: 1324
	Subscribers to Trusted CI email Lists (new)	Continued growth	Announce: 1116 (+272 since previous period) Discuss: 789 (+255 since previous period)
	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 5. All Trusted CI Engagements (in progress and completed) under current award

Engaged Project	NSF Award # or Category	Engagement Subject
Array of Things	1532133	Assisting in crafting a privacy policy and reviewed cybersecurity program
American Museum of Natural History	1547272	Review policies, procedures, and configuration details for securing new Science DMZ.
Cal Poly Pomona SFS	1504526	Assist the Cal Poly Pomona Scholarship for Service Program in providing SFS students experience and training in securing cyberinfrastructure. Provide mentoring to CPP on developing campus cyberinfrastructure, including developing cybersecurity plans.
Cloud Security Best Practices: Agave Platform, Cornell University Center for Advanced Computing, CyVerse, Jetstream (1H2018)	1450437, 1541215, 0735191, 1265383 and, 1445604	Develop cybersecurity best practices for cloud operators.
DataOne	ACI #1430508	Cyber checkup
Design Safe	NHERI: CI-1520817	Cybersecurity review of Design Safe's CI.
DKIST Data Center	AST-0946422	Assisting in the development of an information security program and providing training for staff.
Environmental Data Initiative	NSF DBI Award #1565103 and NSF DEB award #1629233	Reviewed current authentication and authorization mechanisms, identify features and requirements for a future version of the EDI Data Portal and associated backend API, and document currently available authentication and authorization solutions.
FABRIC	1935966 and 2029261	Conducted an asset inventory and risk assessment.
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

Table 5. All Trusted CI Engagements (in progress and completed) under current award (cont)

Engaged Project	NSF Award # or Category	Engagement Subject
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
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

Table 5. All Trusted CI Engagements (in progress and completed) under current award (cont)

Engaged Project	NSF Award # or Category	Engagement Subject
Singularity	1234408, 1547272	In-depth vulnerability assessment (code review) of Singularity.
SLATE	1724821	Supporting development of cybersecurity program.
TransPAC	1450904	Supporting development of cybersecurity program.
UNAVCO		
United States Antarctic Program	Operated by National Science Foundation's Office of Polar Programs	Reviewed processes and policies relevant to polar science information security.
United State Academic Research Fleet (ARF)	1823600, 1824571, 1827383, 1827415, 1827444, 1822574, 1822670, 1824508, 1829214, 1830845, 1823566, 1822532, 1823567, 1823042, 1822954, 1827437, 1822905, 1827654, 1834650	Evaluated existing cybersecurity practices in use across fleet and made recommendations for improvement and to help comply with the IMO 2021 requirements.
University of New Hampshire Research Computing Center	1541430	Assistance in developing an information security program. Quick evaluation of information security program with recommendations for improvement. Training for staff.

Table 6. CTSC (Trusted CI) Engagements under prior award (1234408)

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

Table 6 (continued). CTSC Engagements under prior award (1234408)

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