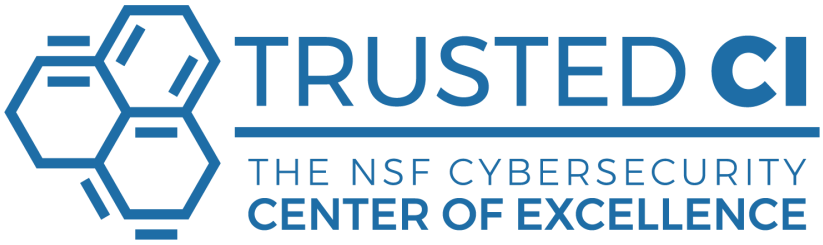


Annual Report for 2023 / Project Year 4

Trusted CI
The NSF Cybersecurity Center of Excellence

NSF Grant ACI-2241313

July 1, 2022 - June 30, 2023

For Public Distribution

Trusted CI Team

Ishan Abhinit,[2] Andrew Adams,[1] Emily Adams,[2] Kay Avila,[3] Jim Basney (PI),[3] Kathy Benninger,[1] Debra Chapman,[6] Diana Cimmer,[2] Adrian Crenshaw,[2] Jeannette Dopheide,[3] Josh Drake,[2] Shane Filus,[1] Terry Fleury,[3] Dan Gunter,[5] Elisa Heymann,[4] Craig Jackson,[2] Ryan Kiser,[2] Mark Krenz,[2] Jim Marsteller,[3] Barton Miller (co-PI),[4] Drew Paine,[5] Sean Peisert (co-PI),[5] Ranson Ricks,[2] Scott Russell,[2] Kelli Shute (co-PI),[2] Mike Simpson,[2] Julie Songer,[2] Alec Yasinsac,[6] John Zage[3]

[1] Carnegie Mellon University/PSC

[2] Indiana University/CACR

[3] University of Illinois/NCSA

[4] University of Wisconsin-Madison

[5] Lawrence Berkeley National Lab

[6] University of South Alabama

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 (TTP) guidance, training and best practices disseminated to the community through webinars, a Fellows program, and the annual, community-building NSF Cybersecurity Summit for Major Facilities (MF) and Cyberinfrastructure.

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

To cite 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 fourth quarter of project year 3 and first three quarters of project year 4, July 1, 2022 - June 30, 2023, of Trusted CI under NSF grant 2241313. Prior to grant 2241313, Trusted CI was supported under NSF grants 1920430, 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.

Trusted CI Annual Report for Project Year 4. July 2023.[1]

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

[1] 10.5281/zenodo.8193570

Trusted CI PY4 Highlights

- The Trusted CI award was transferred from Indiana University to University of Illinois at Urbana-Champaign, and Jim Basney became PI due to Von Welch's departure.
- We attended the 2022 Research Infrastructure Workshop in Boulder, CO and 2023 RIW in DC. For the first event, we delivered a half-day workshop focused on cybersecurity at the Major Facilities (MFs). For the second, we delivered an hour plenary session and 3-hour cybersecurity track.
- We completed both the second and third Framework cohorts ('Bravo' and 'Charlie' cohorts). We established the Trusted CI Framework Community of Practice for cohort 'graduates' to continue building upon the previously established momentum.
- We published version 1.3.3 of the OSCRP, which includes a new section on cloud computing.
- The Annual Challenge team, focused on securing operational technology at NSF Major Facilities, published its initial findings report in July.
- We held the 2022 NSF Summit in October in Bloomington, IN. The post-event attendee survey scores indicated another successful event.
- We graduated our fourth class of Trusted CI Fellows and are excited about their ideas for applying what they learned in their own communities. They provided excellent feedback regarding their experiences and we are applying that feedback to the 2023 program consisting of 7 Fellows.
- The Ambassadors program concluded 2022 with strengthened connections to the Major Facilities. The Ambassadors have played a significant role in recruiting Major Facilities to participate in the Framework Cohorts.
- As an outcome of our 2022 annual challenge, we published our Roadmap for Securing Operational Technology in NSF Scientific Research.
- We completed a First Principles Vulnerability Assessment (FPVA)[2] of the Custos project (NSF award #1840003). We identified five critical vulnerabilities and worked with the Custos team on mitigations.
- The team at University of South Alabama led the first 2-day TTP workshop, which included 13 attendees and presenters.
- Trusted CI was referenced in the NSF Workshop on Infrastructure for AI-enabled cybersecurity: "The National 'Centers of Excellence,' such as Trusted CI, can offer lessons

[2] James A. Kupsch, Barton P. Miller, Eduardo César, and Elisa Heymann, "First Principles Vulnerability Assessment", 2010 ACM Cloud Computing Security Workshop (CCSW), Chicago, IL, October 2010.

to the cybersecurity ecosystem with regards to workforce development, knowledge sharing, and processes required for operating large-scale cyber-infrastructure that enables trustworthy science."

- DoE's report on the ASCR Workshop on Reimagining Codesign[3] referenced Trusted CI's successful model: "Outside of DOE, the National Science Foundation (NSF)'s Office of Advanced Cyberinfrastructure stood up Trusted CI, the NSF Cybersecurity Center of Excellence. The organization has since developed security design patterns for research, including the Trusted CI Framework, a tool to help science and research organizations establish and refine their cybersecurity programs, and the Open Science Cyber Risk Profile, which is listed in a variety of NSF solicitations as a requirement for principal investigators to address in successful proposals. This type of concrete documentation can serve as a valuable resource along with encouragement and mandates from sponsors to ensure this guidance is put into practice. Trusted CI also has a successful fellows program designed to expand the cybersecurity-capable workforce through a guided, hands-on training process. Given the increasing collaboration with the academic community, a partnership with Trusted CI could be invaluable toward expanding DOE's posture and workforce."

[3] https://www.osti.gov/biblio/1822199/

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. Since 2013, Trusted CI has hosted the annual NSF Cybersecurity Summit.[4] The Summit brings together leaders in NSF cyberinfrastructure (CI) and cybersecurity to continue building a trusting, collaborative community addressing the community's core cybersecurity challenges. The 2022 Summit was held in Bloomington, IN. The 2023 Summit will be held October 24-26 in Berkeley, CA.

Progress this year. For the 2022 Summit, the program and organizer committees met monthly to finalize plans. We opened the Summit registration to the public in August with both an in-person and live stream option. The Trusted CI team submitted training. Rob Beverly, NSF program officer, delivered the NSF welcome. Jim Basney gave the State of Trusted CI update. Our keynote speaker, Helen Patton, presented "Cybersecurity: New Issues, Old Problems." Plenary days of the Summit were live streamed to the public. We ran five morning and five afternoon sessions during our training and workshop days. We announced the 2023 NSF Summit, which we are planning to hold in-person in Berkeley, CA at the Lawrence Berkeley National Laboratory October 24-26, 2023. The program chair and co-chair met in January to identify and invite program committee members. The organizing committee kicked off its planning on January 20. Preparation for the 2023 summit so far includes:

- Summit "Save the date" announcement released to the community
- Summit website was created for the 2023 event
- Hotel contract initiated and reservation block selected
- Meeting rooms have been reserved for plenary, training and workshop days

Plans for next year. The program and organizer committees will meet monthly to discuss the Summit. We will open the Summit registration to the public in August with both an in-person and online option.

The Program Committee will develop the Summit program structure and content. This may include a "call for participation" and selection of invited speakers. The Organizer Committee will set up a registration form and open registration to the community.

The Organizing Committee has approved funding for up to 10 student scholarships this year. The call for student applications will be included in the call for participation (CFP).

Planning for the 2024 Summit will begin in January 2024.

[4] https://www.trustedci.org/summit

Metrics.

- CFP response rate: 21 responses to 2022 CFP
- Summit attendee survey responses: 24 of the 42 respondents rated the quality Excellent (highest rating possible); 17 rated the quality Good (second highest rating)
- 23 out of 42 respondents attended in person, 19 participated virtually

1.2 The Ambassadors Program

Background. The Trusted CI Ambassadors Program supports the mission of scientific discovery of the NSF MFs by helping the facilities to establish, evaluate, implement, and evolve their cybersecurity programs, following the methodology established by the Trusted CI Framework. The program assigns one or more Trusted CI staff members as an ambassador to each NSF MF. The program prioritizes efforts to convert the reluctant, *i.e.*, to engage with those facilities that are not already proactively engaging with Trusted CI.

Progress this year. The Ambassadors Program team has continued outreach to their facilities, adding more facilities to subsequent Framework Cohorts throughout PY4. The ’22 Research Infrastructure Workshop at the National Center for Academic Research (NCAR) in September 2022 and the ’23 Research Infrastructure Workshop (RIW) in Washington D.C. provided many opportunities for our ambassadors to make face-to-face connections with numerous facility representatives.

PY4 provided numerous opportunities for our Ambassadors to connect with representatives from the MFs, either in person or virtually:

- 2022 NSF RIW in Boulder, Colorado (September)
- 2022 NSF Cybersecurity Summit in Bloomington, Indiana (October)
- 2022 EDUCAUSE Annual Conference in Denver, Colorado (October)
- 2022 Research Vehicle Technical Enhancement Committee (RVTEC) meeting hosted by University-National Oceanographic Laboratory System (UNOLS) in Seattle, Washington (November)
- 2022 Internet2 Technology Exchange in Denver, Colorado (December)
- 2023 National Institute of Standards and Technology High Performance Computing (NIST HPC) Security workshop panel (March)
- 2023 NSF RIW in Washington, D.C. (June)

Table 1 lists the NSF MFs, assigned Ambassadors, the date the facility joined the Framework Cohort, and the NSF directorate.

Table 1. Major Facilities and Ambassador information

Major Facility	Ambassador	Framework Cohort[5]	NSF Directorate	Recent Interactions
ARF	John Zage	1H2023	GEO	Ryan handed off the Ambassador role to John. Members of ARF attended the Summit in October and RVTEC in November. ARF has attended the Cohort meetings during the reporting period.
Arecibo	Mike Simpson		MPS & GEO	Met in October to discuss ransomware and cloud security. Arecibo ended operations in March. Mike met the project director at the ’22 RIW in September.
Earthscope	Josh Drake	GAGE - 1H2022 SAGE - 2H2022	GEO	GAGE & SAGE attended Cohort meetings during the reporting period and presented on merging cyber programs under Earthscope. Presented at the Summit. The merger has taken up much of their time, Josh acted on an “as needed” basis moving forward.
IceCube	Mark Krenz	1H2023	MPS & GEO	Mark has set up semi-regular meetings with members of IceCube and they are participating in the Cohort. Mark met with a PM at the ’23 RIW in DC.
IODP	John Zage	2H2022[6]	GEO	IODP departed the Cohort due to end of funding as an NSF MF. Their cooperative agreement with NSF ends in 2024.

[5] The “Framework Cohort” column represents the date the facility joined the Trusted CI Framework Cohort. See section 2.7 for more information about the Framework Cohort.
[6] IODP left the Framework Cohort in AUgust 2022

Major Facility	Ambassador	Framework Cohort[5]	NSF Directorate	Recent Interactions
LCCF	Jim Basney	2H2023	CISE	LCCF attended the NSF ’22 RIW in September, met with Jim Basney. Participated in the March 2023 NIST HPC Security workshop panel, moderated by Rob Beverly. LCCF agreed to join the 2H2023 Delta Framework Cohort. Jim made contact with members of LCCF at the ’23 RIW in DC.
LHC ATLAS & CMS	Terry Fleury		MPS	Established a quarterly meeting with US-ATLAS and CMS staff. Met with members of ATLAS team during the Summit and TechEx 2022. Terry has taken over the role as Ambassador and has continued regular contact with the facility.
LIGO	Terry Fleury	1H2022	MPS	Attended Cohort meetings during the reporting period and presented on asset inventories. Continued relationship with Trusted CI through the Framework Cohort CoP meetings.
NCAR	Jim Basney	2H2023	GEO	Met with NCAR staff during September ’22 RIW in Boulder. Bart met with representatives of the NCAR Research Aviation Facility in November to provide advice on software assurance. Participated in the March 2023 NIST HPC Security Workshop panel, moderated by Rob Beverly. Currently participating in the Delta Cohort.

Major Facility	Ambassador	Framework Cohort[5]	NSF Directorate	Recent Interactions
NEON	Ranson Ricks	2H2022	BIO	Attended Cohort meetings during the reporting period. Kay Avila left Trusted CI and handed off Ambassadorship to Ranson. Ranson has met with NEON to manage the transition. Continued relationship with Trusted CI through the Framework Cohort CoP meetings. Connected with Chief Scientist at the ’23 RIW in DC.
NHMFL	John Zage		MPS	NHMFL representatives presented their security program at the Summit. Discussed MagLab's cybersecurity journal article (in preparation), takeaways from the 2022 Summit, and plans to engage with the FSU "Seminole Secure" program.
NOIRLab	Ranson Ricks	1H2022	MPS	Attended Framework CoP meetings and participated in an Ambassador quarterly meeting during the reporting period. Members participated in the Trusted CI panel at the ’23 RIW in DC.
NRAO[7]	Mike Simpson	1H2022	MPS	Attended Framework CoP meetings during the reporting period.
NSO at AURA	Mike Simpson	1H2022	MPS	Attended Cohort meetings and presented on security incidents at NSO. Mike Simpson visited the

[7] For the purposes of project management, The Green Bank Observatory is organized under NRAO and assigned to Mike Simpson.

Major Facility	Ambassador	Framework Cohort[5]	NSF Directorate	Recent Interactions
				site during the ’22 RIW in September. Presented at the Summit. Attended Framework CoP meetings during the reporting period. Contract with ResearchSOC ended, Mike is meeting with NSO quarterly to provide security guidance.
OOI	Andrew Adams	1H2022	GEO	Attended and presented at the Cohort meetings during the reporting period. Presented at the Summit. Attended Framework CoP meetings during the reporting period.
USAP	Mark Krenz	1H2023	GEO	Mark has set up monthly meetings with members of USAP and they have participated in the third Cohort.

Metrics. The Ambassadors Program is tracking the following four metrics:

- Number of MFs with (self-assessed) effective cybersecurity programs: Cohorts 1, 2, and 3 provided self-assessments for seven of 16 of the facilities.
- Number of MFs that have adopted the Framework: 12 of 16.
- Number of MFs with a regular (at least once a quarter) interaction with Trusted CI: 16 of 16 facilities interactions in PY4, including the Framework CoP and the Delta Cohort, as well as phone calls to discuss cybersecurity needs.

Plans for next year. LCCF and NCAR agreed to participate in the 2H2023 Delta Framework Cohort. ATLAS is considering joining the Framework Cohort sometime in 2024. We will establish an outreach plan to bring the MFs into participating at the Summit.

1.3 Other Major Facility Engagement

Background. In addition to the Ambassadors Program (*see* Section 1.2) and the Framework Cohort (*see* Section 2.7), we look for other opportunities to engage with and support the NSF MFs and other key projects. This includes, but is not limited to, collaborating with the Large Facilities Office (LFO).[8]

Progress this year. We hosted a cybersecurity workshop in conjunction with the Research Infrastructure Workshop[9] in Boulder, CO. We collaborated with the LFO to advertise the Summit, taking place in October (*see* section 1.1).

After planning discussions with Richard Oram, Matt Hawkins and Roland Roberts we presented cybersecurity-specific talks at the 2023 Research Infrastructure Workshop (RIW). Trusted CI had a 1-hour plenary slot as well as a 3-hour cybersecurity-specific track during the event.

Plans for next year. We will continue to collaborate with the Research Infrastructure Office to participate in the 2024 RIW and other related events which provide the opportunity for direct connection with MFs and Mid-scale projects.

1.4 Webinar Series

Background. The Trusted CI webinar series[10] 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. PY4 continued to address the concerns of the NSF cybersecurity community. In August, Mark Krenz and Shane Filus gave a presentation on applying the CIS Controls to Trusted CI's cybersecurity program. The purpose of this presentation was to share what we learned from the experience in order to encourage others to apply the controls to their own programs. In September, Carolyn Ellis and Erik Deumens presented on Regulated Research Communities of Practice. Their mission is to build a support network for the people tasked with implementing research compliance in the academic community. Due to the Summit being scheduled in late October, which was the same time we would have hosted a webinar, we did not host a webinar that month. And, because of frequent travel during November and December, we do not present a webinar in November and instead scheduled it in early December before the holidays. Our December webinar detailed our Science DMZ engagement with the University of Arkansas. We spent the remainder of 2022 planning for the 2023 season and booked all but a few of the following season's slots.

[8] https://www.nsf.gov/bfa/lfo/
[9] https://researchinfrastructureoutreach.com/workshop
[10] https://trustedci.org/webinars

The eighth season of the webinar series kicked off with a presentation on securing open source control system software with Professor Gedare Bloom. In February, we welcomed Trusted CI Fellow Rick Wagner to present his experience implementing the Trusted CI Framework at NIH's Common Fund Data Ecosystem. In March, we welcomed Internet2's Steve Wallace to present on routing integrity and upcoming changes to IP registration. In April, Derek Simmel presented a summary of services and support on ACCESS[11], the successor to XSEDE. In May, long-time collaborator Anita Nikolich returned to present on Deception Awareness and Resilience Training (DART). Finally, in June, former member of Trusted CI, Anurag Shankar, presented SecureMyResearch with colleagues Will Drake and Tim Daniel.

It has been very gratifying to see the ripple effects of our community outreach.

Metrics. Table 2 shows the number of webinar attendees and archive viewers in PY4.

Table 2. Trusted CI webinar attendance and archive viewing.

Month	Topic	Speaker(s)	Attended[12]	Watched Later[13]
Aug. '22	CIS Controls w/ Trusted CI	Mark Krenz & Shane Filus	27	58
Sept. '22	Regulated Research Communities of Practice	Carolyn Ellis & Erik Deumens	34	59
Dec. '22	Science DMZ Engagement with University of Arkansas	Mark Krenz, Don DuRousseau, Kathy Benninger	33	86
Jan. '23	Real-Time Operating System and NW Security for Scientific Middleware	Gedare Bloom	34	85
Feb. '23	Security Program for the NIH's Common Fund Data Ecosystem	Rick Wagner	18	39
Mar. '23	Internet2 Routing Integrity and Mutually Agreed Norms for Routing Security (MANRS)	Steven Wallace	21	59
Apr. '23	Advanced Cyberinfrastructure Coordination Ecosystem	Derek Simmel	22	42

[11] Advanced Cyberinfrastructure Coordination Ecosystem (ACCESS): https://access-ci.org/
[12] Does not include Trusted CI staff and presenters.
[13] Viewed later on YouTube.

Month	Topic	Speaker(s)	Attended[12]	Watched Later[13]
	(ACCESS)			
May ’23	Deception Awareness and Resilience Training (DART)	Anita Nikolich	13	48
June ’23	SecureMyResearch	Shankar, Drake, and Daniel	34	56
Total			**236**	**532**

- Webinar registrants added to Announcements mailing list for the reporting period: 49
- Webinar registrants added to the Discuss mailing list for the reporting period: 43

Plans for next year. We will continue to schedule the webinar series, focusing on presenters and topics that impact our community. In the near future, the following webinars have been scheduled:

- July: The Technical Landscape of Ransomware: Threat Models and Defense Models with Barton Miller and Elisa Heymann
- August: Clemson Adaptive Framework with Jeremy Grieshop
- September: Improving the Privacy and Security of Data for Wastewater-based Epidemiology with Stephanie Forrest and Ni Trieu

1.5 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.

- Jim Basney. Research Cybersecurity Insights for 2022. 2022 EDUCAUSE Annual Conference. October 26, 2022. https://hdl.handle.net/2142/115194
- Jim Basney. SC22 MAGIC Meeting: Trusted CI Update. November 15, 2022. https://hdl.handle.net/2142/115844
- Jim Basney. Internet2 Technology Exchange: Trusted CI Update. December 8, 2022. https://hdl.handle.net/2142/116477
- Sean Peisert gave a keynote plenary presentation at the Interdisciplinary Symposium on Responsible Innovation: Intersection of Privacy and Artificial Intelligence, hosted by the Center for Data Science and AI Research (CeDAR) at the University of California, Davis on March 10, 2023: “Usable Computer Security and Privacy Approaches to Enable Data-Driven Analytics and Learning”
- Sean Peisert also sat on a panel at the same symposium: "Responsible Innovation at the Intersection of Privacy and Artificial Intelligence (AI),” with Eric Dang (CA State Senate), Darci Sears (CA State Assembly), Tom Kemp, and Richard Arney.

- Sean Peisert gave a keynote plenary presentation at the 3rd High-Performance Computing Security Workshop[14] on March 16, 2023: "Usable Computer Security and Privacy to Enable Data Sharing in High-Performance Computing Environments."
- Jim Basney presented on the Trusted CI Framework at the 3rd High-Performance Computing Security Workshop on March 15, 2023.[15]
- Jim Basney gave a presentation about Trusted CI at the MS-CC Annual Meeting on May 11, 2023.[16]

1.6 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 to enable deployment of research to improve our national and scientific cybersecurity. Deployment could be in NSF Major or Mid-Scale Facilities, other NSF projects, research computing, commercial entities, government facilities (agency/lab), or academia.

Progress this year. We used our regular interactions with the MFs (through the Ambassadors program and Framework cohort) to discuss their challenges which may benefit from a TTP solution. None were reported or identified this year.

Plans for next quarter. We will continue to leverage our relationships with the MFs to identify TTP opportunities and will communicate those to the research community via our TTP webpage.[17]

1.7 Regional Transition to Practice

Background. The goal of this project is to expand on and complement the efforts of Trusted CI's Cybersecurity Research TTP program by:

1) Building on the University of South Alabama's (USA) previous TTP activities,
2) Establishing a broad and deep footprint of TTP knowledge, best practices, success stories and proponents in the southeast U.S. (Florida, Alabama, Georgia, Mississippi, and Louisiana),
3) Developing a TTP sustainability model that can be replicated in other regions of the United States.

This work complements and extends the goal of TTP in Trusted CI to encourage NSF-funded researchers to transition their research to practice with a set of regionally-focused activities drawing on the USA's existing Industry-University Cooperative Research Centers program. This will be accomplished through promotion and resourcing of TTP engagement to present and future NSF-funded investigators throughout the southeast region of the United States.

---

[14] https://www.nist.gov/news-events/events/2023/03/3rd-high-performance-computing-security-workshop
[15] https://hdl.handle.net/2142/117300
[16] https://hdl.handle.net/2142/118094
[17] https://www.trustedci.org/technology-transition-to-practice

Our TTP activities will serve to promote main goals in connection and collaboration with the Trusted CI Cybersecurity Research TTP program throughout the southeast U.S.:

- Convince NSF Principal Investigators (PIs) of the Value of TTP through the TTP workshops and TTP tutorial sessions
- Facilitate TTP success for investigators that are passionate about transferring their research results
- Support match-making capabilities for potential customers/users with TTP researchers
- Develop best practices for TTP researchers to work through their supporting research offices
- Encourage and enable NSF-funded researchers to transition their research into practice through all of the activities

Progress this year.

- We hosted a virtual introductory workshop on TTP in January, 2023 with 12 attendees. The slideshows and videos of the workshop were posted on both the TTP website and the USA School of Computing website for broader dissemination.
- Created and finalized a handbook on "Working with University Research Offices" which will be posted on the website at the conclusion of the USA Subaward.
- Updated the "Principal Investigator's Guide to Transferring Cybersecurity Technology to Practice (TTP) - Version 2". This will be posted on the website at the conclusion of the USA Subaward

Plans for next year.

- We will host a second virtual worksop on the Future of TTP for Federally Funded Cybersecurity Research in September 2023.
- Creating a contact list of our TTP workshop participants to encourage match-making with TTP researchers

1.8 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[18], blog page views, and unique website visits. **Table 3** 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. Our Twitter impressions have declined compared to the previous year. We attribute this to many users pivoting to alternative platforms. Our blog page views declined as well, we attribute that to publishing fewer blog posts in PY4. Our website visits have held

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

steady. This indicates that our community continues to show interest in our work when we publish content.

Metrics. Table 3 displays our social media impact during PY4.

Table 3. Social media impact during the reporting period

Date	Twitter Impressions	Blog Page Views	Website Visits
July	.7K	4K	.9K
August	1.5K	2.6K	1.5K
September	1.7K	2.6K	1.2K
October	2.6K	2.6K	2K
November	2.5K	3.3K	1.1K
December	1.6K	1.6K	1K
January	.9K	2.8K	.9K
February	.9K	6.7K	1K
March	.9K	2.8K	1.2K
April	.5K	3.5K	1K
May	2K	7.6K	1.1K
June	1.6K	1.7K	1.1K
Total	**17.4K**	**42K**	**14K**
Previous year (for comparison)	58.4K	55.6K	14K

Mailing lists. In addition to tracking activity on websites, we track the number of subscribers to our announcements and discuss mailing lists. In PY4, there were 1123 (-6) subscribers to announcements and 796 (-6) to discuss. We attribute the slight reduction to recently moving our mailing lists to Google groups and removing inactive subscribers.

Plans for next year. We will continue to utilize Blogger, appropriate social media channels, and our website to report our efforts to the public.

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),[19] a community document first developed in 2016 by a working group led by Trusted CI and Berkeley Lab that categorizes

[19] https://trustedci.github.io/OSCRP/

scientific assets and their common risks to science, expedites risk management for open science projects and improves their cybersecurity.

The OSCRP is cited in NSF Research Infrastructure Guide (21-107, December 2021) as well as the Trusted CI Framework Implementation Guide (FIG) as well as numerous NSF CICI solicitations, as indicated below.

The document is a living document and updates are made on an ongoing basis. This effort is led by Trusted CI Deputy Director and co-PI Sean Peisert.

Progress this year. We continued adding operational technology risks as a result of recommendations developed in the 2022 Annual Challenge on Operational Technology and published a blog post to announce an updated version. Additional updates were made to software assurance and operational technology-related sections as a result of the 2021 and 2022 Annual Challenges. A new section on cloud computing was also added. Version 1.3.3 was published in October 2022 with these additions and announced with a blog post in November 2022.[20]

Metrics. Metrics include adoption of the OSCRP and/or related reports by scientific computing projects and continued reference of the OSCRP and/or related reports in funding solicitations and in scientific computing reports and papers.

Mentions and uses of the OSCRP in the last year have included:

- Widespread dissemination to the community, including a 2017 *IEEE Security & Privacy* article (as of July 2023: 826 Full Text Views/Downloads at IEEE Xplore, 134 at CDL).
- Cited in NSF Cybersecurity Innovation for Cybersecurity Infrastructure (CICI) solicitations (18-547, 19-514, 21-512, 22-581, 23-517)
- Trusted CI used in a variety of presentations to Science Gateways (SCGI)
- The OSCRP was used for a non-malicious scientific data integrity threat model, and cited in associated reports and paper at an SC22 workshop:
    - Ishan Abhinit, “Data Integrity Threat Model (Non-Malicious),” 2022. https://scholarworks.iu.edu/dspace/handle/2022/27980
    - Emily K. Adams, “Identifying Malicious Threats to Scientific Data Integrity Using MITRE ATT&CK®,” 2022. https://scholarworks.iu.edu/dspace/handle/2022/28045
    - Trusted CI staff presented a paper at the 17th Workshop on Workflows in Support of Large-Scale Science (WORKS22) at the SC22 conference, highlighting the staff’s recent threat modeling work using the OSCRP: "IRIS: Threat Modeling Scientific Workflow Integrity Using OSCRP and MITRE ATT&CK®" https://scholarworks.iu.edu/dspace/handle/2022/28188
    - Ishan Abhinit, Emily K. Adams, Khairul Alam, Brian Chase, Ewa Deelman, Lev Gorenstein, Stephen Hudson et al. "Novel Proposals for FAIR, Automated, Recommendable, and Robust Workflows." In *Proceedings of the 2022 IEEE/ACM*

[20] https://blog.trustedci.org/2022/11/open-science-cyber-risk-profile-oscrp.html

Workshop on Workflows in Support of Large-Scale Science (WORKS), pp. 84-92. IEEE, 2022. https://ieeexplore.ieee.org/abstract/document/10023942/

- The OSCRP was cited in:
    - James A. Ang, Adolfy Hoisie, Andrew A. Chien, Ian Karlin, Simon Hammond, Scott Pakin, John Shalf, Jeffrey S. Vetter, "Reimagining Codesign for Advanced Scientific Computing Unlocking Transformational Opportunities for Future Computing Systems for Science: Report for the ASCR Workshop on Reimagining Codesign," 16-18 March 2021. https://doi.org/10.2172/1822199

Plans for next year. In 2023, Trusted CI is conducting an Annual Challenge on "security by design" of NSF MFs in the academic maritime and polar domains. We plan to augment the OSCRP with insights from the 2023 study in early 2024.

2.2 Situational Awareness / Cyberinfrastructure (CI) Vulnerabilities

Background. In collaboration with Open Science Grid, the NSF supercomputing centers, and the ResearchSOC, 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, Research Education Networking-Information Sharing & Analysis Center, National Institute of Standards and Technology, and Cybersecurity and Infrastructure Security Agency (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, Globus, and Kubernetes. We also leverage our relationships with the NSF Supercomputing Centers (NCSA, PSC, and other ACCESS service providers). We filter issues for those relevant to the community and then supply simple guidance with those notifications. Trusted CI utilizes 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.[21]

Progress this year. Between July 1, 2022 and June 30, 2023, the Situational Awareness team reviewed 41 vulnerabilities. Of those 41, the team communicated 24 vulnerabilities to the community. In April 2023, the mailing list infrastructure transitioned from Sympa hosted at Indiana University to Google Groups. During the transition, several duplicate and bouncing email accounts were removed from the mailing list.

Metrics. The number of subscribers to the list decreased from 191 as of July 1, 2022 to 190 as of June 30, 2023.

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

[21] https://groups.google.com/a/trustedci.org/g/cv-announce/

2.3 Publications

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

Progress this year.

- Barton P. Miller and Elisa R. Heymann, "The Technical Landscape of Ransomware: Threat Models and Defense Models," Maritime Interdiction Operations Journal, NATO, Issue 24, pp. 20-26, 2022. ISSN 2241-438X.
- D. Yao, S. Rahaman, Y. Xiao, S. Afrose, M. Frantz, K. Tian, N. Meng, C. Cifuentes, Y. Zhao, N. Allen, N. Keynes, B. Miller, E. Heymann, M. Kantarcioglu, and F. Shaon, “Being the Developers’ Friends: Our Experience Developing a High Precision Tool for Secure Coding,” IEEE Security & Privacy, vol. 20, no. 6, November/December 2022, pp. 43-52, DOI 10.1109/MSEC.2022.3159481.
- Elisa R. Heymann, Barton P. Miller, Andrew Adams, Kay Avila, Mark Krenz, Jason R. Lee, and Sean Peisert. “Guide to Securing Scientific Software”, v2.0, June 2023.[22]

2.4 Training

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

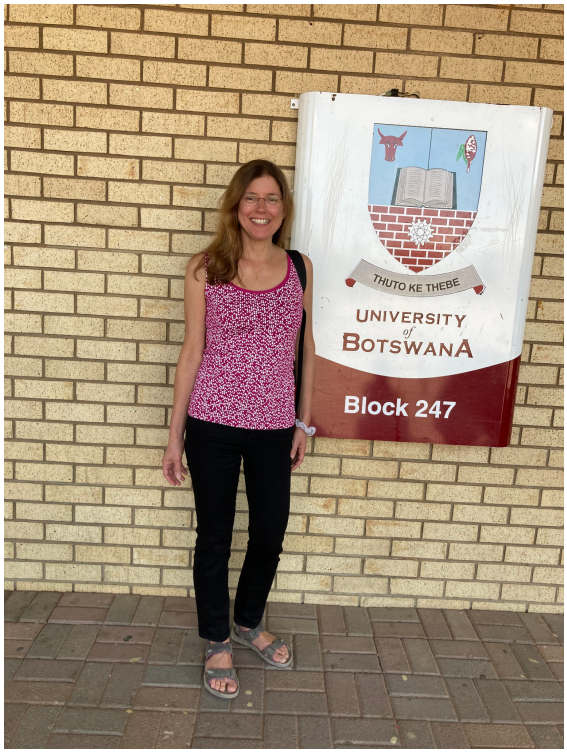
Progress this year. Bart Miller and Elisa Heymann taught an in-person tutorial on Secure Programming and Dependency Analysis Tools at NSF Cybersecurity Summit, in Bloomington, Indiana, in October. The tutorial was a half-day long and included a hands-on segment on web security and dependency tools. They also taught a similar tutorial at Internet2 Technology Exchange, in Denver, Colorado, in December.

In April 2023, Bart Miller and Elisa Heymann taught a three-day tutorial (24 hours total sessions) on Software Security at the University of Botswana, in Gaborone, Botswana.

[22] https://doi.org/10.5281/zenodo.5777646

Images 1 and 2. Heymann and Miller teaching at the NSF Cybersecurity Summit and at Internet2.

Images 3 and 4. Heymann and Miller teaching at the University of Gaborone.



Images 5 and 6. Heymann and Miller teaching at the University of Gaborone.

Mark Krenz and Ishan Abhinit from Trusted CI visited Florida International University[23] in Miami on May 24 through an invitation by NSF ACCESS[24] project (NSF grants #2138259, #2138286, #2138307, #2137603, and #2138296) to conduct a security log analysis workshop for a group of students. Mark and Ishan modified their regular half-day security log analysis[25] workshop and its contents to fit into a two-hour schedule for undergrad students who were from different institutions. The workshop was attended by 15 students. They also provided a brief introduction to cybersecurity careers and shared their experiences on how they entered the field. Later the same day, students were accompanied by Mark and Ishan to their next workshop on 'Sniffing and Password cracking.' Mark and Ishan helped the students complete the exercise and also provided additional insights. Mark also helped the students with more specific cybersecurity questions and concerns about entering the field of cybersecurity.

[23] https://www.fiu.edu/
[24] https://access-ci.org/
[25] https://scholarworks.iu.edu/dspace/handle/2022/23213

Images 7 and 8. Krenz and Abhinit training at NSF ACCESS STEP workshop students at FIU

Plans for next year. We will deliver a series of training sessions at the NSF Cybersecurity Summit, at the 2023 Internet2 Technology Exchange in Minneapolis in September 2023, at Supercomputing '23 in Denver in November 2023. We will continue looking for venues for our training sessions. We also expect to continue teaching at the University of Botswana.

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 CI 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. We presented our work on ransomware at the 6th NATO Maritime Interdiction Operational Training Center Conference on Cyber Security in Maritime Domain at the NATO Souda Base in Chania, Greece, in October 2022. We also taught "Introduction to Software Security" (CS 542) at the University of Wisconsin-Madison (based on UW-Madison instructional funding) using materials developed under Trusted CI. For this class we arranged for our students to take part in a ransomware response cyber tabletop exercise (**Images 9 and 10**) facilitated by the US Department of Homeland Security's CISA, with support from the Wisconsin National Guard Cyber Protection Team, FBI Cyber Investigation Team (Milwaukee), and the Madison Water Utility.[26]

Comments from the students:

> "*I liked the videos that they made on the content and it was easy to follow along with them and understand the material better*". (Note that the videos refer to the material developed under Trusted CI.)
>
> "*The videos were quite helpful. The in-class exercises were also helpful.*"
>
> "*Really loved the class.*"
>
> "*Thank you Professor Miller and Professor Heymann for a great semester. I really enjoyed this class and feel that I got a lot out of it.*"
>
> "*Overall, well taught. Thank you for the good semester!*"
>
> "*This class was amazing*."

[26] https://www.cs.wisc.edu/2022/11/23/new-cyber-academic-cooperation/

Images 9 and 10. Tabletop exercise

In addition, we continued working on our study of ransomware and a comprehensive report on our findings. Miller presented a ransomware briefing at the Wisconsin National Guard Joint Forces Headquarters in November, based on this Trusted CI effort.

Bart Miller and Elisa Heymann continued producing teaching material, available at https://research.cs.wisc.edu/mist/SoftwareSecurityCourse/. The new material includes four new book chapters: 3.9.1. Web Attacks: Background, 3.9.2 Web Attacks: Cross Site Scripting, 3.9.3 Web Attacks: Cross Site Request Forgery, 3.9.4: Web Attacks: Session Management; and three new online modules on dependency tools, Address Space Layout Randomization, and Memory Safety Checks.

As an ongoing activity, we completed the version 2.0 of the Guide to Securing Scientific Software, including major updates to these sections:

- 3.5 Software Supply Chain
- 3.6 Insecure Design
- 4.5 Software Analysis Tools

And introduction of three new sections:

- 4.3 Secure Design
- 4.6 Fuzz Testing
- 4.7 Code Auditing

The Guide to Securing Scientific Software 2.0 is ready for community release in July 2023.

We also conducted research on a technical taxonomy and landscape for ransomware and produced a report on these efforts for community use. This report is ready to be released in July 2023.

Metrics.

- Two papers published.
- One technical report.
- Three new online modules on dependency tools, Address Space Layout Randomization, and Memory Safety Checks.
- Four new book chapters on Web Attacks: Background, Web Attacks: Cross Site Scripting, Web Attacks: Cross Site Request Forgery, and Web Attacks: Session Management.
- 180 students registered for the "Introduction to Software Security" course (two sections) taught in the Spring 2023 semester at the University of Wisconsin-Madison.
- Download statistics:
    - Text chapters and papers: 28,366
    - Hands-on exercises and instructions (note that our base virtual machine contains almost all the exercises): 7848
    - Video views: 3,437

Plans for next year. Prepare material to teach two sections of our "Introduction to Software Security" course in fall at the University of Wisconsin-Madison. We are also working on the Table Top exercise, which will simulate the response to another ransomware attack, this time on our local power grid. In addition to DHS, Wisconsin National Guard, and FBI, we will have support from the U.S. Department of Energy and a couple of companies who specialize in cyber defenses for the energy section.

Release our report on ransomware in multiple forms and venues. These forms include a detailed technical version, a list of best practices, and an executive-manager policy summary.

2.6 Continuing Professional Education

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. Trusted CI CPEs are distributed in the form of badges, currently issued through Badgr,[27] an open source badge issuing website. Badgr has features that allow recipients to share their badges on social media[28] (LinkedIn, Facebook, Twitter, etc.).

Progress this year. In PY4 we hosted nine webinar events that qualified for CPE badges. We issued 2022 badges to the Trusted CI Fellows. And we issued badges to 2022 Summit attendees.

Metrics. The following badges were issued during PY4:

- PY4 Webinars: 309
- 2022 Fellows: 8
- 2022 Summit Plenary: 140

[27] Trusted CI Badgr page: https://badgr.com/public/issuers/EhlDU1W_TnmOs8lD4O_j8A/badges
[28] https://support.badgr.com/en/knowledge/sharing-badges-on-social-media

- 2022 Summit trainings/workshops: 143

Plans for next quarter. We will continue to issue badges for qualifying events.

2.7 The Trusted CI Framework: An Architecture for Cybersecurity Programs

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. During this period of performance, the Framework Team continued to execute the Trusted CI Framework Cohort program; initiated a new engagement strategy for post-Cohort graduates; and started the process of building a Trusted CI Framework Cohort reassessment approach.

Trusted CI Framework Cohort: In January 2022, Trusted CI initiated the Framework Cohort program. This six-month, group engagement approach has proven effective facilitating adoption and implementation of the Trusted CI Framework among NSF MFs. The program is beginning to have an impact as some organizations are initiating changes to their cybersecurity programs during the engagement. We also had strong Mid-scale representation in the Charlie Cohort.

Trusted CI has graduated three Cohorts since inception of the program. Cohorts Bravo and Charlie completed the engagement during this period of performance, and include the following organizations:

Organization	Type
Academic Research Fleet (ARF)	Major Facility
The Corporation for Educational Network Initiatives in California (CENIC)	Regional Network
Deep Soil Ecotron (DSE)	Mid-scale
FABRIC	Mid-scale
Giant Magellan Telescope (GMTO)	Other
IceCube Neutrino Observatory (IceCube)	Major Facility
The National Ecological Observatory Network (NEON)	Major Facility
Network for Advance NMR (NAN)	Mid-scale

Seismological Facility for the Advancement of Geoscience (SAGE)[29]	Major Facility
US Antarctic Program (USAP)	Major Facility

Trusted CI Framework Community of Practice (CoP): Trusted CI initiated the Framework Community of Practice (CoP) in January 2023 to advance implementation of the Trusted CI Framework among Cohort graduates and continue to build on the relationships fostered during the Cohort engagements. The Cohort project is achieving its intended outcome of scaling Framework adoption, and now the CoP is helping NSF MFs and Mid-scales continue a path toward fully implementing the Framework.

Trusted CI structured the CoP as a member-led program facilitated by the Framework team. Members conduct quarterly workshops / meetings that will lead to achieving measurable outcomes. We conducted the inaugural workshop in March that was well received by Alpha and Bravo Cohorts, and we will welcome Charlie Cohort at the July workshop.

Framework Reassessment Initiative: Trusted CI initiated a program to reassess the cybersecurity programs of facilities that have completed a Cohort or similar engagement over time. The goal of these reassessments is to track the progress of MFs and Mid-scales as they establish and refine their cybersecurity programs. We began by conducting a lightweight pilot reassessment of NOIRLab following their one-on-one Framework Engagement with Trusted CI in 2021. Our planned approach is to reengage with Cohort graduates individually every two to three years to gauge progress, identify new challenges, and propose new ratings. These reassessments are planned to be short (1-2 hours), focused on validating the updated self-assessment of the facility. As part of this reevaluation, Trusted CI will draft a new Validated Self-Assessment Report, with updated ratings for each of the 16 Framework Musts, and new strategic priorities for the organization to pursue over the subsequent two-to-three- year period.

Framework Broader Impacts. The Trusted CI Framework is being used beyond the boundaries of the NSF community. For example, the State of Indiana has formally adopted a subset of the Framework Musts for its local government cybersecurity assessment program. Also, the number of Framework adopters has grown beyond just NSF MFs. CENIC, Indiana University OmniSOC, the GMTO, and the NIH Common Fund Data Ecosystem are among the organizations adopting the Framework. Finally, Jim Basney and Craig Jackson met with NIST to brief them on the Framework.

Metrics.

- More than 60 percent of NSF MFs have adopted the Trusted CI Framework
- 15 organizations completed the Cohort program
- Launched the CoP initiative

[29] Now part of EarthScop Consortium, https://www.earthscope.org/

Plans for next year.

- Complete Delta Cohort
- Evaluate and consider revisions to the FIG
- Continue to buildout the CoP program
- Develop a Trusted CI Framework Reassessment Program.

2.8 Broader Impacts

Background. Trusted CI is charged with addressing cybersecurity challenges affecting small projects, multi-institution collaborations, international collaborations and MFs. While we engage directly with NSF projects (via engagements, summits, webinars, mailing lists), we also focus on how to develop and implement strategies which help meet the cybersecurity needs of a broader set of NSF projects (both small and large) and to provide demonstrated value to a significant percentage of NSF projects. In addition, we work with other communities to train, assess, and advise organizations on relevant topics, including the Trusted CI Framework.

Progress this year. We continued to update our metrics regarding impact across NSF divisions.

Metrics. Our metrics are captured in **Images 11** and **12**.

Image 11. Chart of total NSF directorate impact

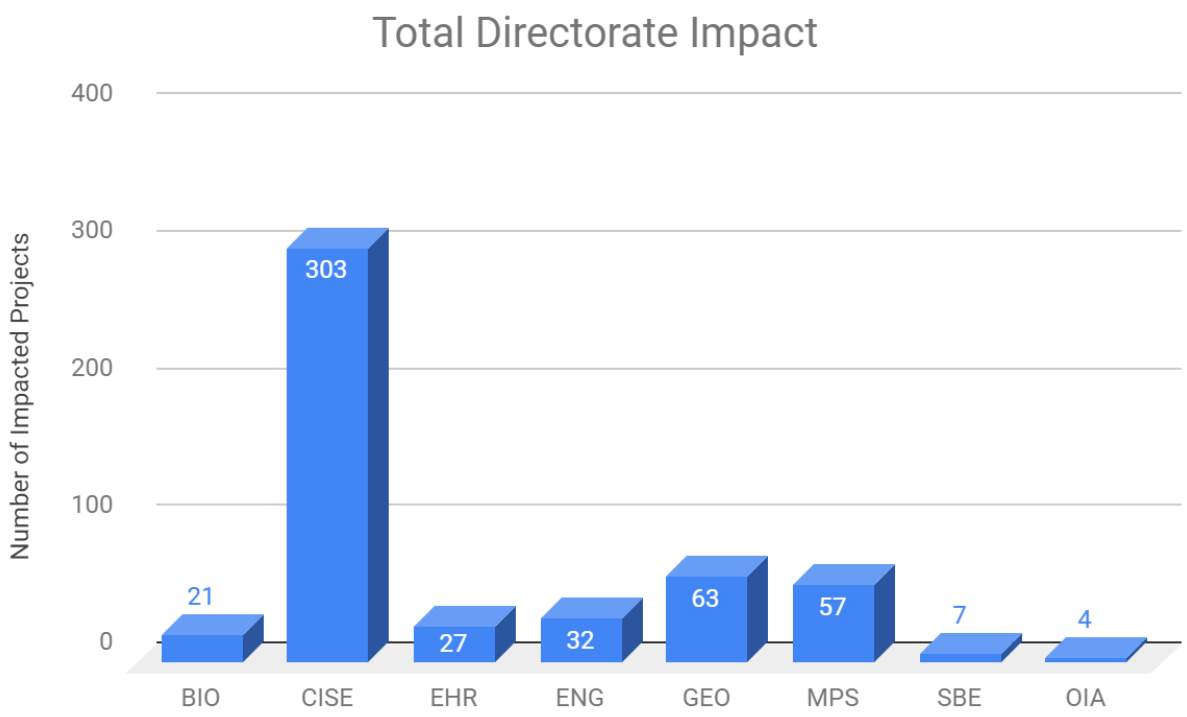
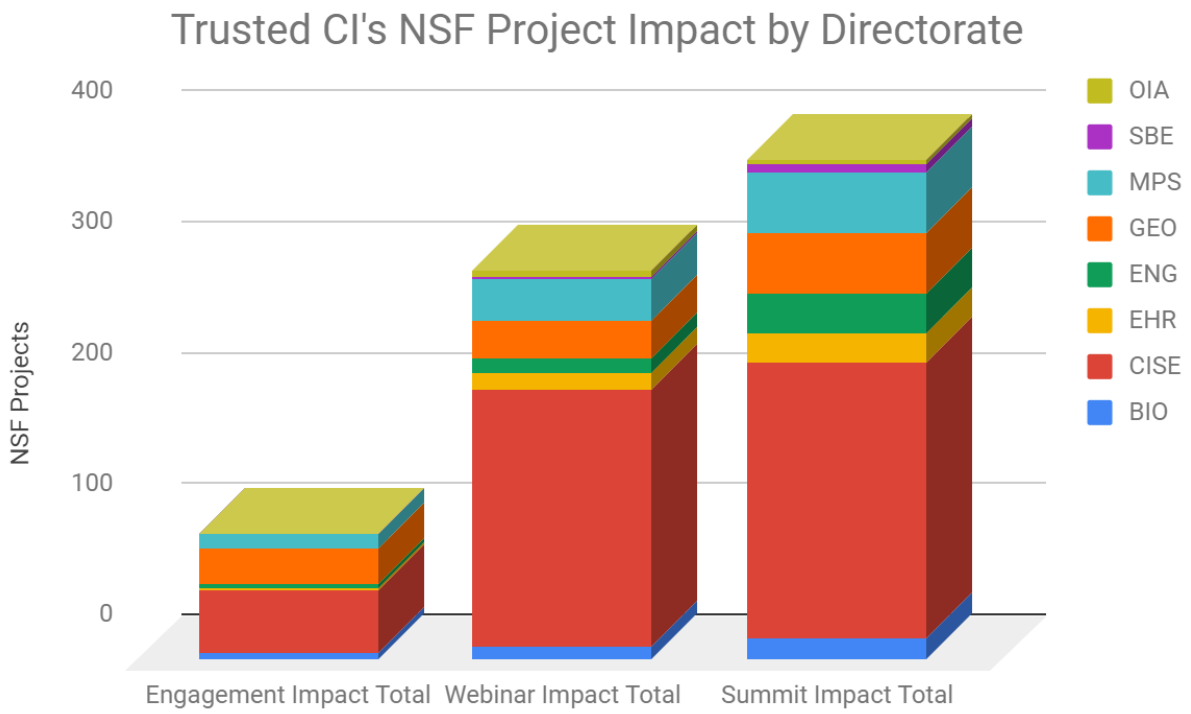


Image 12. Chart of NSF project impact by directorate and activity type



Plans for next year. Continue to update metrics from the Summit as well as webinars as they occur, as well as gathering metrics from the participants of Framework Cohorts.

2.9 Fellows Program

Background. On an annual basis, Trusted CI solicits applications from and selects 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 2022 class of Fellows completed their weekly virtual institute sessions and participated on a panel at the NSF Summit (four in person and four via video). All eight Fellows graduated and were presented with plaques as recognition for their contributions to the program. The Call for Applications for the 2023 Fellows Cohort was announced at the 2022 Summit. We ranked and selected the 2023 Fellows. We notified applicants of our decisions on February 24 and engaged with the accepted Fellows to plan and kick off our interactions and their participation in other Trusted CI projects. We had an in-person kick off at EDUCAUSE CPPC, with a meet and greet dinner with four Fellows and two other guests. The virtual institute program began in May with guest speakers.

Plans for next year. Trusted CI Fellows will continue the weekly virtual institute sessions, with guest speakers. Among the speakers will be Kent Wada on privacy, Scott Russell on cybersecurity programs and the Trusted CI Framework, Craig Jackson on Risk & Risk Acceptance. Four Fellows will attend Practice and Experience in Advanced Research Computing (PEARC). The Fellows will participate on a 30-minute panel at the NSF Summit. All seven Fellows will graduate and will be presented with plaques as recognition for their contributions to the program. The Call for Applications for the 2024 Fellows Cohort will be announced at the 2023 Summit. After that time the applications will be reviewed by the Advisory Committee, Fellows alumni, and the Trusted CI team. Six new Fellows will be chosen to kick off the 6th Cohort of Trusted CI Fellows.

2.10 Law and Policy Insights

Background. The IU Center for Applied Cybersecurity Research (CACR) 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. The Law and Policy Insights project focuses on the development of in-depth guidance on particularly complex or salient issues facing the community: specifically, General Data Protection Regulation compliance and the Cybersecurity Maturity Model Certification. These in-depth guidance materials 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 2H 2022 the Law and Policy project had three student affiliates, who developed memoranda relating to: 1) ADPPA, a pending privacy law in Congress; 2) a summary of state PII laws; and 3) an introduction to data brokers. In 1H 2023, the Law and Policy project had two student affiliates who developed memoranda relating to artificial intelligence regulation and ransomware. Additionally, the project lead presented on the artificial intelligence research at a CACR Privacy and Security Luncheon.

Plans for next year. The Law and Policy Project will onboard additional student affiliates for the fall 2023 semester and spring 2024 semester.

2.11 Annual Challenges

Background. In calendar-year 2020, then-Trusted CI deputy director and co-PI Jim Basney led a community study on trustworthy data, leading to a public findings and solutions document. In calendar-year 2021, Trusted CI embarked on an Annual Challenge that sought to broadly improve the robustness of software used in scientific computing with respect to security. It also delivered a findings document as well as a "Guide to Secure Software" intended to be a living document maintained by Trusted CI. The 2021 effort was led by Trusted CI co-PI Sean Peisert.

In calendar-year 2022, Trusted CI examined the security of operational technology (or cyber-physical systems) used in science. This included control systems as well as sensor systems. We spent the first half of 2022 engaging with operators of cyber-physical systems in science to

understand the range of operational practices and evaluate potential deficiencies that lead to vulnerabilities and compromises. In the second half of 2022, we leveraged our insights to develop a multi-year roadmap of solutions to advance security of scientific operational technology. This effort was led by Trusted CI deputy director and co-PI Sean Peisert.

Progress this year. The 2022 Annual Challenge Team published its findings report in July 2022 along with an accompanying blog post.[30]

> Emily K. Adams, Daniel Gunter, Ryan Kiser, Mark Krenz, Sean Peisert, Susan Sons, and John Zage. "Findings of the 2022 Trusted CI Study on the Security of Operational Technology in NSF Scientific Research," July 13, 2022. DOI: 10.5281/zenodo.6828675 https://doi.org/10.5281/zenodo.6828675

A plenary presentation at the NSF Cybersecurity Summit in October 2022 was given.[31] We finished and published the solutions roadmap document and announced publication via Trusted CI email lists, a blog post,[32] and social media.

> Andrew Adams, Emily K. Adams, Dan Gunter, Ryan Kiser, Mark Krenz, Sean Peisert, and John Zage. "Roadmap for Securing Operational Technology in NSF Scientific Research," November 16 2022. DOI: 10.5281/zenodo.7327987 https://doi.org/10.5281/zenodo.7327987

The 2023 Annual Challenge is engaging with MFs undergoing construction and refreshes in a hands-on way to build security in — particularly with respect to operational technology — from the outset.[33] Trusted CI is directly supporting the planning for facility refreshes or construction with respect to both information and operational technology. Our focus in 2023 is "ships and poles." This ties directly into the Ambassadors program and, in some cases, also 2023 Framework Cohorts. Specifically, in 2023, Trusted CI is engaging with the Scripps Institution of Oceanography team designing the California Coastal Research Vessel (CCRV),[34] the team at Oregon State University (OSU) that supported the design and construction of the Research Class Research Vessels (RCRVs),[35] and the Ocean Observatories Initiative (OOI) team overseeing the refresh of their autonomous underwater vehicle and glider fleet. (The CCRV and RCRVs are expected to join the U.S. Academic Research Fleet (ARF).) Recently, this has included site visits of the ARF's R/V *Sally Ride* and OSU's Hatfield Marine Science Center in Newport, Oregon, where the R/V *Taani* — one of the initial three RCRVs being constructed — will be based upon completion of its construction. The *Sally Ride* visit resulted in important insights about cybersecurity perspectives of marine technicians.

---

[30] https://blog.trustedci.org/2022/07/findings-of-2022-trusted-ci-study-on.html
[31] https://www.youtube.com/watch?v=mkFsk4LEF68
[32] https://blog.trustedci.org/2022/11/publication-of-trusted-ci-roadmap-for.html
[33] https://blog.trustedci.org/2023/01/announcing-2023-trusted-ci-annual.html
[34] https://scripps.ucsd.edu/news/naval-architect-selected-uc-san-diegos-new-california-coastal-hybrid-hydrogen-research-vessel
[35] https://ceoas.oregonstate.edu/regional-class-research-vessel-rcrv

The U.S. Antarctic Program (USAP) teams designing the Antarctic Research Vessel (ARV)[36] and supporting the USAP land facilities refreshes (McMurdo, Palmer, and Amundsen-Scott South Pole stations) are also supporting Trusted CI's insights into the challenges and best practices in this domain. This has included productive engagements with USAP personnel at the NSF RIW in Washington, D.C.

We are also having conversations with stakeholders connected with academic maritime activities, including UNOLS personnel, marine technicians, scientists who use these facilities (*e.g.*, oceanographers), and software developers connected with oceanographic data collection. We are also pursuing conversations with additional teams, who may be added to this list as the effort moves forward into calendar year 2024, including Arctic facilities and other ships in the ARF.

Recent site visit photographs:

Image 13. Trusted CI's Sean Peisert in a crawlspace on the R/V *Sally Ride* examining operational technology systems.

[36] https://future.usap.gov/arv/

Image 14. The R/V *Sally Ride*, docked in Alameda, CA.

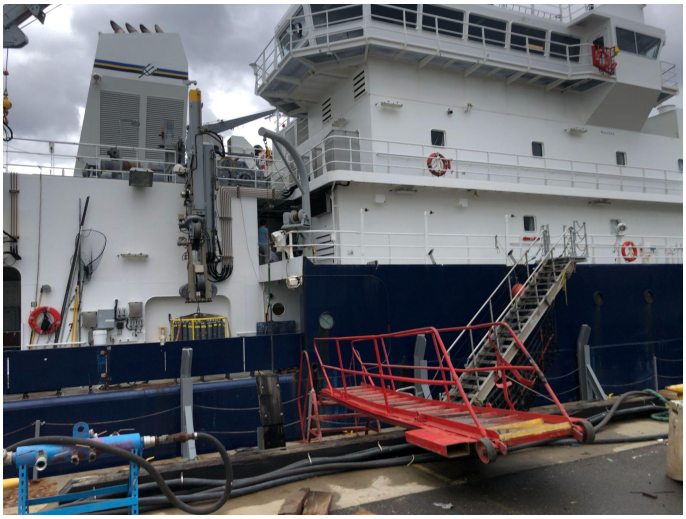
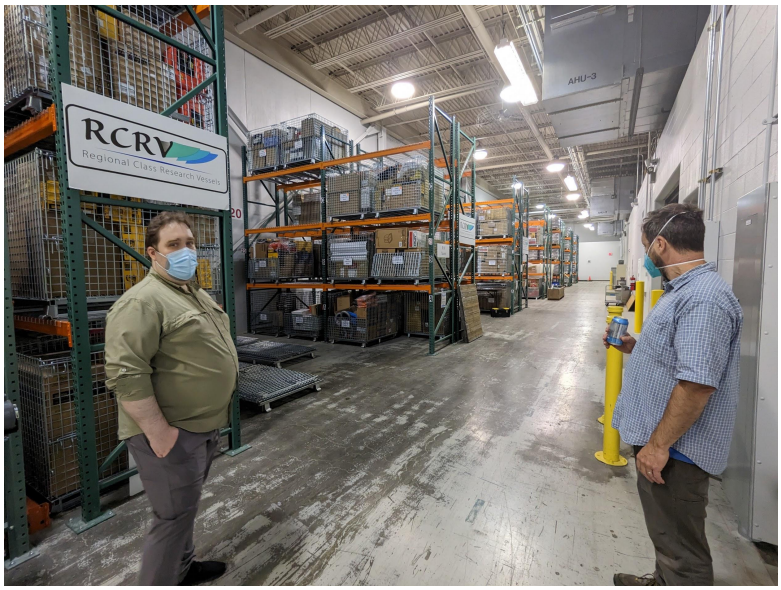


Image 15. Trusted CI's Dan Arnold conferring with marine technicians on the R/V *Sally Ride*.

Image 16. Trusted CI's John Zage, left, looks on as RCRV's Chris Romsos, right, explains some of the scientific instruments that will be part of the newly constructed ships at the RCRV's offices at OSU, Corvallis, OR.

Image 17. Trusted CI's John Zage left, and RCRV's Chris Romsos, right, view part of the expansive warehouse of items and gear to outfit the new ships under construction. OSU, Corvallis, OR.



Metrics. As with the 2021 Annual Challenge, for the 2022 and 2023 Annual Challenges, many of the metrics will also be measured in future years, as they relate to adoption and impact, which takes time. For 2022's metrics, we can state that five MFs (IceCube, NOIRLab, OOI, United States ARF, USAP) covering three NSF divisions (Geosciences (GEO)/Ocean Sciences (OCE), GEO/Office of Polar Programs (OPP), and MPS/Astronomical Sciences (AST)) chose to work with us. These

divisions also happen to be the largest sponsors of the MFs by far, and so while only three divisions are covered, they actually represent a significant majority of NSF's total MFs by both quantity, funding amounts, and numbers of end users. For the 2023 Annual Challenge, we are working with four MFs (OOI, Research Class Research Vessel Construction, United States ARF, USAP) in which GEO/OCE is also represented by three MFs that Trusted CI is directly supporting while USAP in GEO/OPP is providing valuable research insight. Finally, we note that we have met all milestones.

The 2023 Annual Challenge has already demonstrated success in bringing together previously disparate groups of ARF institutions (e.g., operations, project management, system administrators, and security) to discuss cybersecurity needs when designing new ships. It has also brought cross-institution teams together to share lessons learned between institutions at different stages of design and construction.

On a technical level, the Annual Challenge has helped with formalization and documentation of testing procedures and configuration changes. These procedures will be used after construction is complete to allow ship operators to have updates and configuration changes vetted before they are applied in production in order to increase the ship operators' confidence that applying them will not result in unexpected results or errors. In turn, this will allow ship operators to more regularly apply updates and test configuration changes, including those to mitigate vulnerabilities, in a more timely manner.

Finally, the Annual Challenge has developed initial lists of cybersecurity-related questions and criteria to use when speaking with vendors about procurements.

Plans for next year. The 2023 Annual Challenge will continue to engage with the CCRV, OOI, and RCRV design teams. It will also continue to interact with the USAP team to continue to better gain insights that can support security by design of academic maritime ships specifically and MFs more broadly. We will also continue to develop plans for site visits as needs arise. We will also continue to have stakeholder discussions and will continue pursuing conversations with additional teams, who may be added to the effort. We plan to have a workshop on this subject at the 2023 NSF Cybersecurity Summit[37] or in a subsequent webinar later in 2023. The 2023 Annual Challenge will continue into CY 2024.

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 CI projects and MFs through collaborative engagements that address specific project needs. Trusted CI engagement activities

[37] https://www.trustedci.org/2023-cybersecurity-summit

include (but are not limited to) security reviews, security architecture design, identity management, 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 quarter. We continue to offer direct engagement with the MFs via our Framework adoption Cohort and Ambassadors program. We will continue to monitor the success of the Cohort approach and consider offering one-on-one engagements once all NSF MFs have adopted the Framework (or expressed a reason why they do not wish to do so).

Metrics. N/A

Plans for next quarter. Standard one-on-one engagements will remain on hold as we facilitate the Framework Cohorts in their stead (*see* section 2.7)

3.2 Custos Engagement

Background. Trusted CI collaborated with Indiana University to assess the security of the Custos system.[38] The Custos framework provides common security operations for science gateways. Custos capabilities include user identity and access management, gateway tenant profile management, resource secrets management, and groups and sharing management.

Progress this year. We applied our First Principles Vulnerability Assessment (FPVA) methodology to perform an in-depth assessment of Custos. We generated architectural and resource diagrams containing information on privileges and reviewed all the diagrams with the Custos team. When performing the component analysis step of FPVA, we found five critical vulnerabilities. For each of those vulnerabilities, we wrote a vulnerability report and discussed the mitigations with the Custos team. Additionally, we generated a list of bugs that affect the Custos system.

We delivered the final engagement report and it was accepted by the Custos team. They were extremely satisfied with the results of our engagements. Their exact words were:

> *"We greatly appreciate the due diligence. This is an incredibly useful analysis for our group, the first of its kind. We also hope to cultivate some of the lessons learned in other software products we develop."*

3.3 Office Hours Consultations

Background. Trusted CI offers office hours consultations by appointment on 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) and other cybersecurity topics of interest to NSF projects. Understanding that many cybersecurity topics cannot be addressed in just one

[38] https://airavata.apache.org/custos/

hour, the office hours can generate follow-up activities, such as blog posts, engagements, and webinars.

Progress this year. We delivered the following consultations this year:

- USAP archival team: In August Mark Krenz met with the team that manages science data that comes out of Antarctica for long-term archival. Although they aren't directly part of USAP, they are related to the science there and Mark was able to help provide them some cybersecurity guidance and agreed to a quarterly meeting.
- Craig Jackson consulted with National Radio Astronomy Observatory (NRAO) on cyber insurance.
- Bart Miller and Elisa Heymann consulted with representatives of the NCAR Research Aviation Facility. We provided background on our online software security training materials, and different forms of engagement. They chose to look at the online materials by themselves and will contact us if they have questions.
- Jim Basney consulted with Karan Vahi (ISI) about identity management for https://www.nimhgenetics.org/ (with assistance from Erik Scott from CI Compass), including a discussion of content for the next revision of the "Federated Identity Management Cookbook."[39]
- Sean gave an interview to RAND staff about a study they're doing on the DHS Centers of Excellence. As a component of a larger effort to understand the core functions needed for COEs and related long-term planning processes, the RAND staff were looking for best practices and lessons learned from Trusted CI in terms of its function, operation, and relationship with its constituent communities that they could potentially leverage to help improve the DHS Centers of Excellence going forward.

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

4 Lessons Learned, Challenges, and Project Management

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

4.1 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 team meeting
- Engagement with the Advisory Committee
- Budgeting/overseeing spending

[39] https://ci-compass.org/resource-library/publication-the-federated-identity-management-cookbook/

- 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. We completed the transition of the award from Indiana University to University of Illinois-Urbana Champaign. The new award is 2241313. In addition, we submitted a request to change the PI from Von Welch to Jim Basney.

We delivered quarterly reports on schedule as well as a Program Execution Plan at the beginning of the calendar year. We continue to monitor the program for significant changes warranting an update to or amendment of the PEP.

We attended a meeting, facilitated by Advisory Committee member Damian Clarke, with representatives from HBCUs. We learned about the challenges they face with respect to cyberinfrastructure and how Trusted CI can be of service to this community.

We created a draft of our new five-year strategic vision. That vision has been distributed to key community members, including our Advisory Committee and Framework Community of Practice members. The vision will ultimately feed into our renewal proposal. We finalized all project plans for 2023 and monitor progress against those plans on a monthly basis.

Lastly, we began planning for our upcoming 48-month review. We collaborated with NSF to select a date for the review, reviewed materials from our 30-month review panel, and developed a project plan to track milestones and progress.

Plans for next year. We will continue to deliver all program reports to NSF on our established schedule. We will participate in a 48-month review with an NSF-selected review panel, release our 5-year strategic vision for public comment, and submit a 5-year renewal proposal to NSF.

4.2 Advisory Committee Changes and Meeting

Background. The Trusted CI Advisory Committee serves to provide Trusted CI with strategic guidance. While 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
- Neil Chue Hong, Director of the Software Sustainability Institute
- 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[40].

Progress this year. We held our final Advisory Committee meeting of 2022 in November. Our March 8 scheduled Advisory Committee meeting was unfortunately lightly attended with conflicts emerging at the last minute. With the members who were able to attend, we discussed opportunities to further Trusted CI's diversity and inclusion as well as scaling our impact.

The leadership team discussed an alternate approach to engaging with our AC members which resulted in a series of one-on-one meetings between Director Basney and AC members. This provided the opportunity for more direct and transparent feedback regarding emerging challenges and our upcoming renewal proposal.

Plans for next year. We will reassess our meeting frequency and approach, considering whether or not the reintroduction of a once-yearly in-person meeting is an effective solution to the challenges faced when convening this team. We will reevaluate membership and identify if new members are warranted, especially in light of our revised vision.

4.3 Trusted CI All Team Meeting

Background. Each year, we hold the Trusted CI all team meeting, an opportunity for the team 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. We held an in-person all team meeting in Chicago on August 9 and 10, 2022. This was our first in-person meeting since March 2020. The meeting provided opportunities for networking and relationship building. We began planning the 2023 ATM taking place in August.

Metrics. 31 staff attended both virtually and in person

Plans for next year. We will hold an in-person all team meeting in Chicago on August 23 and 24. We will preview the 48-month review presentation and solicit feedback from across the team. We will begin planning for the 2024 all team meeting, selecting a date and reserving the Big Ten Conference Center.

4.4 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

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

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 finalized and delivered the PEP for calendar year 2023.

Plans for next year. We will monitor the project for any changes warranting a formal update to the PEP and deliver an updated version to NSF if warranted. We will deliver a new PEP for 2024 in January.

4.5 Personnel Changes

The following personnel changes occurred during the reporting period:

- Indiana University (CACR) - In July 2022, Von Welch departed IU's CACR and accepted a position at NCSA. He has since departed his position at NCSA. Trusted CI's executive director, Kelli Shute, became the IU site lead and co-PI representing the project. Adrian Crenshaw and Emily Adams left the team in January.
- Lawrence Berkeley National Laboratory - Sean Peisert, who had been a Trusted CI co-PI and the Berkeley Lab Site Lead, also took on the role of Trusted CI deputy director. Jason Salinas joined the Berkeley Lab team to support NSF Cybersecurity Summit organization.
- Pittsburgh Supercomputing Center - Hawa Na Aata, an IT security analyst/engineer, joined the team in January.
- University of Illinois (NCSA) - In July 2022, Von Welch took a short-term position at NCSA to assist with the award transfer from Indiana to Illinois. Jim Basney, formerly deputy director and co-PI, replaced Von as Trusted CI's PI and director. After assisting with the award transfer from Indiana to Illinois, Von Welch's short-term position with Trusted CI at NCSA ended in September 2022. Kay Avila left the team in January 2023. Jim Marsteller joined the team in January 2023 to assist with planning for the 2023 Summit.
- University of South Alabama - none
- University of Wisconsin - Benjamin Nibbelink and Calvin Kranig, both graduate students joined Trusted CI in September 2022 for the Custos engagement. Both left after the engagement finished due to graduating with their MS degrees. Sai Chaparala and Gia-Minh Nguyen, both undergraduate students, joined Trusted CI in May 2023 to work on the upcoming Tapis engagement.

4.6 ResearchSOC Collaboration

Background. While Trusted CI and ResearchSOC have distinct roles in the NSF ecosystem (Trusted CI is a trusted, technology-neutral cybersecurity leader and consultant, and the ResearchSOC delivers 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 5.7)

- Alignment of ResearchSOC security and operational metrics with the Trusted CI Framework (*see* Section 2.7)
- Outreach: ResearchSOC presents to the NSF community (*see* Section 1.1) and at Trusted CI-hosted events (PEARC and the NSF Cybersecurity Summit).

Progress this year. We continued our quarterly meetings between Trusted CI and ResearchSOC leadership to discuss additional opportunities for collaboration and cross-promotion of events. As Trusted CI focuses on MFs and the ResearchSOC takes on more MF clients, the coordination has increased, including sharing the increasing knowledge about the MFs between the projects through Trusted CI's Ambassadors Program. We invited Susan Sons, Director of ResearchSOC, to present at the RIW during the cybersecurity track. She also joined the new class of Fellows at EDUCAUSE CPPC to provide insights into her career in cybersecurity and to answer questions regarding their challenges and topics of interest.

Metrics. Seven points of collaboration.

Plans for next year. We will continue our leadership series. Kelli will no longer be an active ResearchSOC team member; therefore, the leadership series and maintaining our ongoing connection and collaboration with intention will be that much more important.

4.7 Trusted CI Cybersecurity Program

Background. Trusted CI maintains its own cybersecurity program 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. Our primary effort this past year was in the design, preparation, and implementation of moving our Trusted CI data assets from our old personal Google 'My Drive' account (vonwelch.com) to a Google shared drive using a domain-based account (TrustedCI.org). This endeavor involved:

- procuring the domain-based service at Google;
- re-registering our DNS domains to be under that Google account;
- developing policy to govern use of the new shared drive focusing on mitigating over-sharing;
- educating staff in that policy and appropriate workflows in the new shared drive;
- and finally, effecting the migration of our data.

Moreover, since we were experiencing issues in managing the various mailing lists Trusted CI used through IU's Mailman application, we also leveraged Google's Groups and Google Workspace mailing list solutions to migrate management of many of our mailing lists too.

A second major task we undertook was the process of addressing the 'unacceptable' ratings we received during a self-assessment of our implementation of the CIS Controls we're using as a baseline control set to protect our information assets. Although less than 20 of the 180 controls in the CIS Controls failed our self-assessment, the majority of those were addressed by adding additional security features, *e.g.*, MFA, segmentation/isolation and pursuing staff cybersecurity awareness options. There are, however, five remaining unaddressed controls, but we have identified solutions for those and expect to complete our enhancement of those early in our next year of operation.

Plans for next year. As alluded to above, we expect to complete our effort of addressing all 'unacceptable' CIS Controls ratings from our self-assessment. We will also perform our annual review of all our policy documents, including an audit that our security program documents are up to date on our website. Additional policy and controls -- specifically for our data assets -- will be explored to expire data assets (again, in an effort to mitigate against over-sharing), and to ensure that our data does not have PII within. Similarly, we intend to guide the development of CloudPerm in order to have it audit the share settings used with our Google shared drive, such that we can then periodically poll project leads to ensure those settings are correct. Finally, we plan to utilize our upcoming annual face-to-face all-team meeting as a venue to provide cybersecurity awareness to staff.

5 International Travel and Impact

During PY4, the Trusted CI team undertook no international travel under Trusted CI funding. Mike Simpson, Ambassador to Major Facilities, will attend the NMIOTC Cybersecurity Conference[41] in September 2023, supported by Trusted CI funding.

[41] https://nmiotc.nato.int/transformation/conferences/cyber-security-conference/