
# Annual Report for Project Year 5

# Trusted CI
# The NSF Cybersecurity Center of Excellence

NSF Grant OAC-2241313

July 1, 2023 - September 30, 2024

For Public Distribution

Trusted CI Team

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

[1] Carnegie Mellon University/Pittsburgh Supercomputing Center (PSC)

[2] Indiana University/Center for Applied Cybersecurity Research (CACR)/OmniSOC

[3] University of Illinois/National Center for Supercomputing Applications (NCSA)

[4] University of Wisconsin-Madison

[5] Lawrence Berkeley National Laboratory

[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 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 Peisert, 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 annual report of project year 5,[1] July 1, 2023 through September 30, 2024, of Trusted CI under NSF grant 2241313. Prior to this, 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.



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

[1] Our prior annual report concluded on June 30, 2023. As such, this report covers an additional quarter (July 1, 2023 - September 30, 2023) in addition to PY5.

# Trusted CI Annual Highlights

- We hosted a successful four-day 2023 NSF Cybersecurity Summit at the Lawrence Berkeley National Lab in October.
- Bart Miller and Elisa Heymann taught a tutorial on Secure Programming and Dependency Analysis Tools at the 2023 Internet2 Technology Exchange in Minneapolis in September 2023.
- The second TTP workshop led by University of South Alabama was held in September 2023. That event marked the completion of the USA subaward with Trusted CI.
- Mike Simpson, Bart Miller, and Elisa Heymann attended the 7th NATO Maritime Interdiction Operational Training Center Conference on Cyber Security in Maritime Domain at the NATO Souda Base in Chania, Greece.
- We completed the fourth and fifth Framework adoption cohorts. Cohort Delta consisted of high performance computing centers. Cohort Echo had strong representation from NSF Mid-scales. Graduates of both cohorts completed the program with their final self-assessment and draft Cybersecurity Program Strategic Plans.
- We held quarterly workshops for the Research Infrastructure Security Community (RISC), the first was in conjunction with the Summit.
- We supported the October launch of the Minority Serving Cyberinfrastructure Consortium (MS-CC) Cybersecurity Community of Practice. Jim Basney, Sean Peisert, Damian Rouson, and Kelli Shute attended the quarterly meetings, which are well attended by MS-CC member institutions.
- We completed a successful engagement with Tapis, discovering four significant vulnerabilities for the Tapis team to address. We published a success story about our engagement with the project.[2]
- We received an "Excellent" rating from our 48-month NSF review panel.
- Much of the Trusted CI team attended the Research Infrastructure Workshop (RIW[3]) in Tucson in March. Trusted CI participated in the cybersecurity-specific track with Craig Jackson presenting the Transformative Twelve. Trusted CI RISC members participated in a panel on effective cybersecurity programs and Wade Craig presented a summary of NRAO's cybersecurity history and program development.
- Secure by Design team members continued their efforts related to the OT Procurement Vendor Matrix. Progress included drafting a guide to using the matrix and receiving feedback from a maritime vendor. They also presented a poster at the RIW, winning second place in the competition.

[2] https://doi.org/m92p
[3] https://researchinfrastructureoutreach.com/

- Drew Paine represented Trusted CI at the CICI PI meeting in Tempe in March.
- 13 of 14 NSF Major Facilities (MFs) have now completed the Trusted CI Framework Cohort program, with the one remaining NSF MF scheduled for 2025.
- We opened the call for participation for the 2024 Summit student program and selected 19 attendees from the 208 student applications that we received. We invited a student from the 2023 program to attend and facilitate a capture the flag with the 2024 class of students.
- Trusted CI personnel met with NSF's Laura Stolp to discuss OCE's CI/CS plans.
- In coordination with OmniSOC, we retired our CI Vulnerabilities service, replaced by the new OmniSOC Community Advisory newsletter.
- We co-authored a research paper on ransomware accepted for the 2024 IEEE International Conference on Cyber Security and Resilience (IEEE CSR).
- We taught half-day tutorials on Secure Programming and Dependency Analysis Tools at the 2023 NSF Cybersecurity Summit and Supercomputing '23.
- We engaged with each of the members of Trusted CI's new Advisory Committee (AC) to confirm their availability to attend an AC kickoff meeting in conjunction with the 2024 NSF Cybersecurity Summit.
- We held two in-person All Team meetings in Chicago at the Big Ten Conference Center.
- Sean Peisert visited the R/V *Sally Ride* as part of a "cyber update day" while *RIDE* was in port. *RIDE* is an "ocean-class" vessel based at the Nimitz Marine Facility at Scripps Institution of Oceanography (SIO) and is part of the U.S. Academic Fleet. The visit included a ship tour, a view of the systems being patched/updated, inspections of the ship's bridge, server, multi-beam sonar, science, and engine rooms, and an inspection of the new satellite domes that had recently been installed.

# 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 2024 Summit will be held October 7-10 in Pittsburgh, PA.

**Progress this year.** We held the 2023 Summit in person in Berkeley, CA at the Lawrence Berkeley National Laboratory and offered a streaming option for virtual attendees. The Summit, held on October 23-26, included plenary, workshops/training, and (new this year) a poster session. We had 191 in-person registrants and 137 virtual registrants. The conference had an overall attendance of 173 people in-person throughout the event, with an overall virtual attendance of 55 attendees. On the first full day, we had Zeek training and Jupyter workshops. On day two, Rob Beverly, NSF program officer, delivered the NSF welcome. Jim Basney gave the State of Trusted CI update and Sean Peisert and Adam Slagell delivered a Berkeley and ESNet welcome. Our keynote speaker, Aunshul Rege, presented "Social Engineering Manifestations as Ransomware Attacks Unfold" and plenary sessions and workshops followed in the afternoon. Days three and four were a mix of plenaries and workshops/trainings.

We began planning for the 2024 Summit. The Program Committee conducted a community poll to determine the topics they'd like to see addressed. The top topics were incorporated into the Call for Participation (CFP) to steer proposals for talks, workshops, training and Birds of a Feather (BoF). We received 30 responses to the CFP. The Program Committee continued to review possible keynote speakers and plenary panel sessions. We also solicited submissions for the Summit student program and received applications from 208 students, the highest number of applications ever received for the program. The Organizing and Program Committees have finalized the logistics for the Summit. The event will take place in Pittsburgh, PA, at Carnegie Mellon University October 7-10, 2024. For those unable to attend in person, virtual streaming options will be available. The Summit will feature plenary sessions, workshops/trainings, and poster sessions. Currently, we have 170 in-person registrants and 110 virtual registrants. The agenda for the event includes a full day of Zeek training on day one, a welcome address from NSF on day two, a welcome from CMU/PSC, and an update from Sean Peisert on Trusted CI. Dr. Lorrie Faith Cranor will be the keynote speaker, presenting on "Security and Privacy for Humans." The afternoons will be filled with workshops and trainings. Days three and four will feature a mix of plenary sessions and workshops/trainings.

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

**Metrics.**

Registration totals (2023):

- In-person - 191
- Remote - 137

## 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 NSF Cybersecurity Summit in October provided numerous interactions with our contacts at the MFs. We spent the last months of 2023 strategizing how to bring EarthScope, LHC's CMS, and MagLab into the Framework Cohort.

In March, the Ambassadors participated in the NSF RIW. Prior to the workshop, the ambassadors reached out to their contacts at the MFs to encourage them to attend the workshop, if not in-person, then virtually. Some ambassadors had prior commitments and coordinated with those who attended in-person, tasking them with following up on various security-related topics at the facility. Ambassadors also participated in the RISC quarterly workshop the day before the RIW began.

We presented a review of the Ambassadors project at the April Trusted CI All Team call. We attended the fourth High-Performance Computing Security Workshop at Wichita State University. More details about the individual facilities can be found in the table below.

**Table 1.** NSF MFs and Ambassador Information

| Major Facility | Ambassador | Framework Cohort[5] | NSF Directorate | Interactions |
|---|---|---|---|---|
| ARF | John Zage | 1H2023 | GEO | Secure by Design team wrapped up the vendor questionnaire matrix, thanks to input from CCRV and RCRV. John and Ryan Kiser met internally to discuss milestones for ARF in 2024. John has taken over the ambassador role to ARF. Mikeal Jones has assumed the role of virtual CISO for ARF |

[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.

| Major Facility | Ambassador | Framework Cohort[5] | NSF Directorate | Interactions |
|---|---|---|---|---|
| | | | | and is in routine contact with John. ARF went through on-site inspections, infosec audits, ransomware drills, and other security-related activities in the reporting period. Members of ARF will be attending the 2024 Summit. |
| EarthScope | Josh Drake | GAGE - 1H2022<br>SAGE - 2H2022 | GEO | Contact with EarthScope is somewhat limited since the GAGE & SAGE merger. But, EarthScope named Trusted CI in its proposal as a line item in their budget. They had a retreat in July, but unfortunately Josh could not attend. Another one is planned for later in 2024. Members of EarthScope will be attending the 2024 Summit. |
| IceCube | Mark Krenz | 1H2023 | MPS & GEO | Meeting monthly with IceCube to touch base and address any security concerns they have. IceCube attended the RIW, including the RISC quarterly meeting. Secure by Design hosted a call with Steve Barnet to discuss all things secure by design. This has turned into a proposed BoF on cyber insurance at the 2024 Summit. |
| LCCF | Jim Basney | 2H2023 | CISE | LCCF (TACC) participated in the Framework cohort during the reporting period. Jim attended the HPC security workshop at Wichita State. LCCF has secured its next round of funding. Members of LCCF will be attending the 2024 Summit. |
| LHC ATLAS & CMS | Terry Fleury | | MPS | Remained in regular contact with the CMS side of the project. Attended the High Throughput Computing workshop at UW-Madison in July and established |

| Major Facility | Ambassador | Framework Cohort[5] | NSF Directorate | Interactions |
|---|---|---|---|---|
| | | | | contacts with new ATLAS representatives. Both ATLAS and CMS are planning to participate in a 2025 Cohort. |
| LIGO | Terry Fleury | 1H2022 | MPS | LIGO is a member of the RISC and attended the quarterly meetings during the Summit and the RIW. Members of LIGO will be attending the 2024 Summit. |
| NCAR | Mark Krenz | 2H2023 | GEO | NCAR (UCAR) participated in the Framework cohort during the reporting period. Mark has taken over as NCAR ambassador and met the facilities contact at the RIW. Members of UCAR will be attending the 2024 Summit. |
| NEON | Ranson Ricks | 2H2022 | BIO | NEON was not able to attend the 2023 Summit. Ranson met later to discuss what was missed. And, cybersecurity has been added as a line-item in their budget, this has been credited to Trusted CI. Ranson has requested an alternate contact with NEON due to limited availability. Members of NEON will be attending the 2024 Summit. |
| NHMFL (MagLab) | John Zage | 1H2024 | MPS | Members of MagLab attended the 2023 Summit. They joined the cohort in 1H2024. Our security contact at MagLab was not able to attend the RIW. Members of MagLab will be attending the 2024 Summit. |
| NOIRLab | Ranson Ricks | 1H2022 | MPS | Members of NOIRLab attended the 2023 Summit and the RISC quarterly meetings at the 2023 Summit and the RIW. They also complimented Trusted CI during their presentation on a recent cybersecurity incident. Members of NOIRLab will be attending the 2024 Summit. |

| Major Facility | Ambassador | Framework Cohort[5] | NSF Directorate | Interactions |
|---|---|---|---|---|
| NRAO[6] | Josh Drake | 1H2022 | MPS | Attended RISC meetings during the reporting period. Josh took over the ambassador role in 2024. Our NRAO security contact attended the RIW remotely, including the RISC quarterly meeting. Due to the departure of David Halsted in April, Josh is coordinating with NRAO on their cybersecurity leadership transition. Wade Craig from NRAO is actively participating in the Summit Program Committee. |
| NSO at AURA | Josh Drake | 1H2022 | MPS | Attended RISC meetings during the reporting period. Josh took over the ambassador role in 2024. Our NRAO security contact attended the RIW, including the RISC quarterly meeting. |
| OOI | Andrew Adams | 1H2022 | GEO | Attended RISC meetings during the reporting period. Received positive feedback on the vendor questionnaire produced by the Secure by Design team. Participated in the panel at the Summit. Our OOI security contact attended the RIW, including the RISC quarterly meeting. Andrew met with OOI to discuss the outcome of a security survey and work to address the gaps identified in the review. Members of OOI will be attending the 2024 Summit. |
| USAP | Mark Krenz | 1H2023 | GEO | Monthly meetings with members of USAP. Received positive feedback on the vendor questionnaire produced by the Secure by Design team. Participated in the panel at the 2023 Summit. Members of USAP will |

[6] 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 | Interactions |
|---|---|---|---|---|
| | | | | participate in the 2024 Summit next month, including the panel. |

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

- Number of MFs that have adopted the Framework: 13 of 14.
- Number of MFs with a regular (at least once a quarter) interaction with Trusted CI: 14 of 14 facilities interactions in PY5, including the Framework CoP and cohort, as well as phone calls to discuss cybersecurity needs

## 1.3 Other Major Facility Engagement

**Background.** In addition to the Ambassadors Program (*see* Section 1.2) and the Framework cohort (*see* Section 2.9), 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 Research Infrastructure Office (RIO)[7] and CI Compass.[8]

**Progress this year.** We collaborated with the RIO to plan the cybersecurity-specific content at the 2024 RIW. We also continued a discussion with Mike Corn (NFS's Cybersecurity Advisor For Research) regarding the most effective cybersecurity controls applicable to research infrastructure operators. CI Compass and Trusted CI leadership met monthly to coordinate on MF support activities.

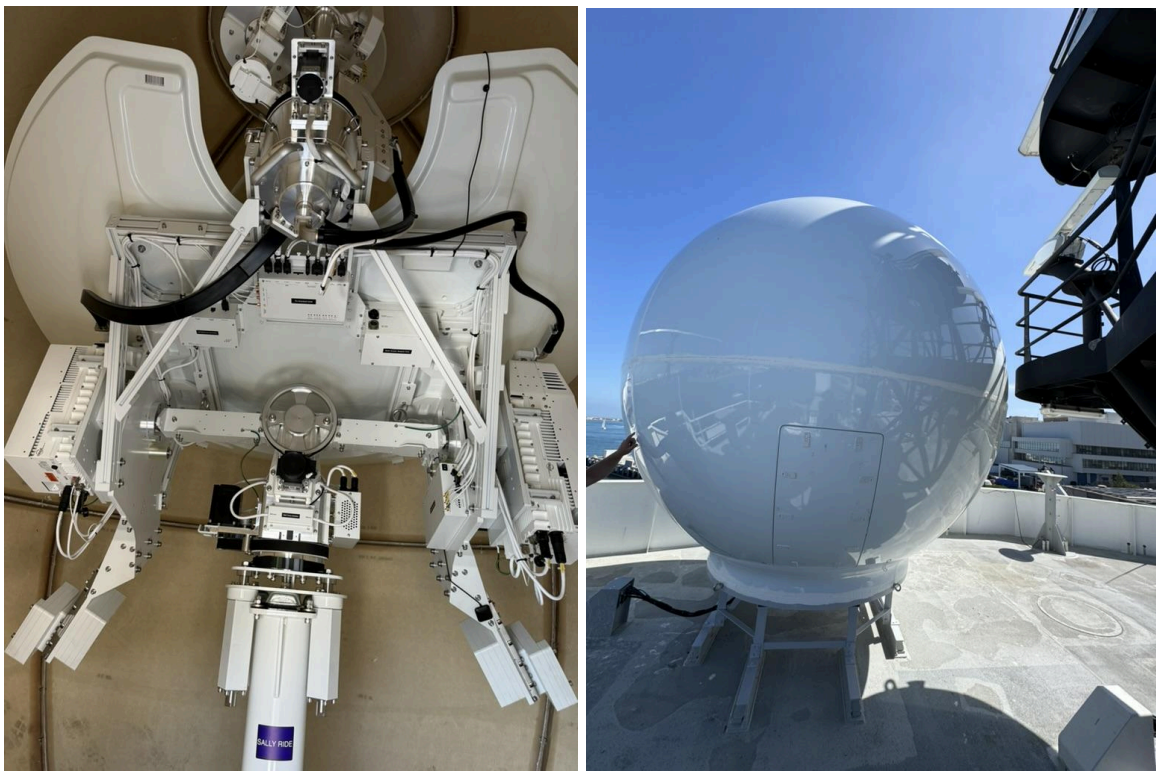
Program leadership attended the CI4MF workshop in Long Beach, CA, where many MF representatives were in attendance (*see* section 1.5). We further developed relationships with facility and NSF program leadership at the RIW hosted by NSF in Tucson. The RIW provided opportunities to learn more about the upcoming changes to the Research Infrastructure Guide (RIG) and other activities underway being led by Mike Corn. We established a regular meeting series with Mike to stay abreast of those initiatives and their potential impacts on MFs. Drew Paine attended the 2024 NSF CICI PI meeting in Tempe, AZ.

We will continue to identify opportunities to deepen connections with MF representatives. Our regular meetings with Mike Corn will continue, and we'll look for opportunities to contribute to the RIG revisions based on our experiences collaborating with NSF MFs. Trusted CI personnel met with NSF's Laura Stolp in June to discuss OCE's CI/CS plans going forward and ways in which Trusted CI could support that. We plan regular future meetings as well. We will continue to coordinate with Richard Oram of the RIO to support development of the cybersecurity agenda for the 2025 RIW and to incorporate relevant talks into Trusted CI events, such as the annual Summit.

[7] https://www.nsf.gov/bfa/lfo/
[8] https://ci-compass.org/

Sean Peisert visited the R/V *Sally Ride*[9] in Point Loma, San Diego, CA, on August 14, 2024 as part of a "cyber update day" while *RIDE* was in port. *RIDE* is an "ocean-class" vessel based at the Nimitz Marine Facility[10] at Scripps Institution of Oceanography (SIO) and is part of the U.S. Academic Fleet.[11] Peisert was hosted by Jon Meyer and Lee Ellett of the SIO, UC San Diego. The visit included a ship tour, a view of the systems being patched/updated, inspections of the ship's bridge, server, multi-beam sonar, science, and engine rooms, and an inspection of the new satellite domes that had recently been installed (see **Image 1 and 2**, below).

**Images 1 and 2.** Photos from the recent site visit to the R/V *Sally Ride.*



## 1.4 Webinar Series

**Background.** The Trusted CI webinar series[12] 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.** In early December, Subhashini Sivagnanam presented "Enhancing Integrity and Confidentiality for Secure Distributed Data Sharing (Open Science Chain)." In March, Ron

[9] https://scripps.ucsd.edu/ships/sally-ride
[10] https://scripps.ucsd.edu/ships/marine-facility
[11] https://www.unols.org/ships-facilities/unols-vessels/unols-designated-vessels/unols-designated-vessels
[12] https://trustedci.org/webinars

Hutchins and Tho Nguyen presented “Lesson from the ACCORD Project.” In April, we had a team presentation on SPHERE (Security and Privacy Heterogeneous Environment for Reproducible Experimentation) from Jelena Mirkovic and David Balenson. In May, NSF’s Mike Corn presented the upcoming publication of the RIG. In June, Trusted CI’s Craig Jackson presented The Transformative Twelve, which focused on evidence-based approaches to cybersecurity controls for projects of any size. In July, Mike Dopheide presented a webinar on Zeek build and deployment testing. In August, Trusted CI’s Jim Basney co-hosted a presentation with Derek Weitzel on JSON Tokens and Jupyter Notebooks. Note: there were some presenter cancellations over the year, which accounts for the gaps in the dates.

**Metrics. Table 2** shows the number of webinar attendees and archive viewers in the reporting period, including a count of self-reported unique NSF project affiliations among attendees ("Impacted Projects").

**Table 2.** Trusted CI webinar attendance and archive viewing.

| Month | Topic | Speaker(s) | Attended[13] | Watched Later[14] | Impacted Projects |
|---|---|---|---|---|---|
| July | Ransomware Landscape | Barton Miller & Elisa Heymann | 24 | 24 | |
| Aug. | Clemson Adaptive Framework | Jeremy Grieshop | 15 | 35 | |
| Sep. | Securing Data Wastewater-based Epidemiology | Ni Trieu | 11 | 28 | |
| Dec.[15] | Enhancing Integrity and Confidentiality for Secure Distributed Data Sharing (Open Science Chain) | Subhashini Sivagnanam | 10 | 50 | 4 |
| Mar. | Lessons from the ACCORD Project | Ron Hutchins, Tho Nguyen | 32 | 159 | 5 |
| April | SPHERE | Mirkovic & Balenson | 20 | 36 | 1 |
| May | NSF Research Infr. Guide | Mike Corn | 28 | 84 | 7 |
| June | Transformative Twelve | Craig Jackson | 26 | 57 | 3 |
| July | Zeek Automation | Mike Dopheide | 24 | 40 | 2 |
| August | JSON Tokens & Jupyter Demo | Jim Basney & Derek Weitzel | 17 | 93 | 5 |
| Total | | | 157 | 519 | 27 |

[13] Does not include Trusted CI staff and presenters.
[14] Viewed later on YouTube: https://youtube.com/playlist?list=PLLoFSG1hhthQNMernoG1yT1yxeYnWkGYP&si=9XxM_ok0k9-hY9YS
[15] Due to frequent travel during November and December, we do not present a webinar in November and instead schedule it in mid-December before the holidays.

- Webinar registrants added to Announcements mailing list for the reporting period: 54
- Webinar registrants added to the Discuss mailing list for the reporting period: 43

## 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.

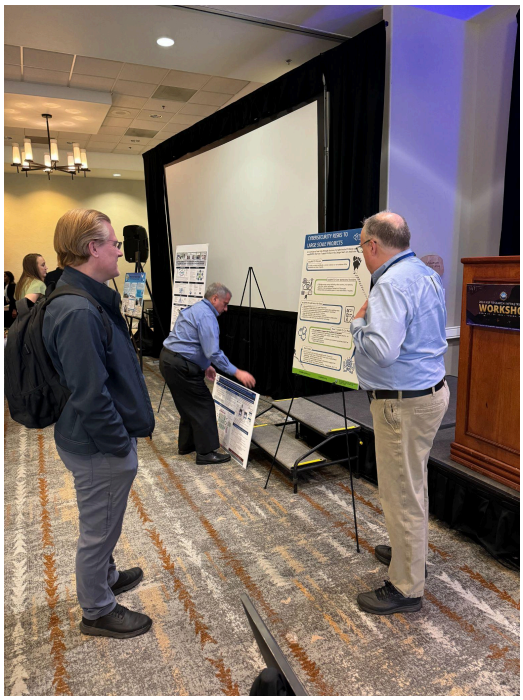
**Progress this year.** Trusted CI team members attended and presented at the following events this year:

- Jim Basney presented “The Trusted CI Framework for Cybersecurity Programs” at the MS-CC All Hands Meeting, August 24, 2023.
- Sean Peisert presented “"Trustworthy Scientific Cyberinfrastructure" at the NASEM Cyber Resilience Forum Summer Meeting, San Francisco, CA, August 31, 2023.
- Bart Miller and Elisa Heymann presented their work on code authorship identification at the 7th NATO Maritime Interdiction Operational Training Center Conference on Cyber Security in Maritime Domain at the NATO Souda Base in Chania, Greece, in September 2023.Sean Peisert, “Usable Computer Security and Privacy to Enable Privacy-Preserving Computing on Sensitive Health Data” (invited expert panelist), Workshop on Secure Methods for Sharing Health Data, California Council on Science and Technology (CCST), Sacramento, CA, Dec. 7, 2023.
- Jim Basney, Sean Peisert, and Kelli Shute attended the CI Compass-hosted CI4MF[16] event in January. PI Basney presented a lightning talk updating the community on Trusted CI’s recent activities and accomplishments. Of particular interest to the community was the recently-released Vendor Procurement Matrix, a product of our Secure By Design initiative (*see* section 2.11).
- Much of the Trusted CI team attended the RIW[17] in Tucson in March. Trusted CI participated in the cybersecurity-specific track with Craig Jackson presenting the Transformative Twelve. Trusted CI RISC members participated in a panel on effective cybersecurity programs and Wade Craig presented a summary of NRAO’s cybersecurity history and program development. The Secure by Design team presented a poster during the conference poster session. (*See* **Images 3 and 4**.)
- Mark Krenz from Trusted CI presented a two-hour workshop on Linux security best practices to the NSF ACCESS STEP (NSF #2138307) program participants, which included 14 undergraduate and two graduate students from 15 institutions of higher education, including one Historically Black Colleges and Universities institution.
- Sean Peisert presented “Trustworthy Scientific Cyberinfrastructure” at the Federal Cybersecurity R&D Interagency Working Group (CSIA IWG), NITRD, May 23, 2024.

[16] https://ci-compass.org/news-and-events/events/2024/01/18/ci4mf-2024-collaboration-in-action/
[17] https://researchinfrastructureoutreach.com/

**Image 3.** Craig Jackson presents the Transformative Twelve at the RIW.


**Image 4.** Mark Krenz presents the Secure by Design poster at the RIW poster session.



## 1.6 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 U.S..

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 is accomplished through promotion and resourcing of TTP engagement to present and future NSF-funded investigators throughout the southeast region of the United States.

Our TTP activities 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 quarter.**

- We completed the "Working with University Research Offices" guidebook and posted on the USA TTP website along with the Trusted CI TTP website.
- We completed version 2 of "A Principal Investigator's Guide to Transferring Cybersecurity Technology to Practice (TTP)". This guide was posted on the USA TTP website along with the Trusted CI TTP website.
- We hosted the 2nd virtual workshop on the Future of TTP for Federally Funded Cybersecurity Research on Sept. 14th-15th, 2023. We had 93 registered participants and 30 attendees. The workshop materials have been posted to the USA TTP website along with the Trusted CI TTP Website. All registered participants were provided links to the workshop materials.
- Workshop participants were provided with contact information for all participants to encourage match-making with TTP researchers.

**Plans for next quarter.** This subaward ended on September 30, 2023.

## 1.7 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 blog page view, unique website visits, LinkedIn subscribers, and mailing list subscribers. **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.** We saw a notable increase in blog page views compared to the previous year, but it appears primarily due to bots from outside the USA. Website visits compared to the previous year have held steady. We also officially transitioned to LinkedIn as our primary social media platform for disseminating program information.

**Metrics. Table 3** displays our social media impact during Y5Q1.

**Table 3.** Social media impact during the reporting period

| Date | Blog Page Views per month | Website Visits per month | LinkedIn Follower Count |
|---|---|---|---|
| July | 11.1K | 1.1K | |
| August | 27.3K | 1.6K | |
| September | 2K | 2K | |
| October | 4.4K | 2.1K | |
| November | 8.2K | 1.1K | |
| December | 2K | .9K | |
| January | 7.2K | 1.8K | |
| February | 8.7K | .9 | |
| March | 8.7K | 1K | 88 |
| April | 9.5K | 1K | |
| May | 19.9K | 1.4K | |
| June | 19.2K | 1.6K | 92 |
| July | 37.2K | 1.3K | |
| August | 31.5K | 1.7K | |
| September | TBD | 1.2K[18] | |
| **Total** | **196.9K** | **20.7K** | **99** |
| Previous year[19] | 55.6K | 14K | N/A |

**Mailing lists**. In addition to tracking activity on websites, we track the number of subscribers to our announcements and discuss mailing lists. In the reporting period, there were 1141 (+18) subscribers to announcements and 825 (+29) to discuss.

[18] This is the total as of the creation of the report (prior to the end of the project year).
[19] This row shows the totals for the same period in the previous year, for comparison.

## 1.8 MS-CC Partnership

**Background.** Trusted CI partners with the Minority Serving Cyberinfrastructure Consortium (MS-CC) on community building related to cybersecurity for cyberinfrastructure at minority serving institutions. Trusted CI co-organizes the MS-CC Cybersecurity Community of Practice (CCoP) and provides cybersecurity content for MS-CC workshops, webinars, and events.

**Progress this year.** Trusted CI supported the October launch of the MS-CC CCoP, which provides a monthly forum for community-driven experience sharing to support and raise awareness of and best practices related to CI cybersecurity at HBCUs, TCUs, and other MSIs for faculty, researchers, staff, and students.[20] PI Basney also participated in the MS-CC Cybersecurity Workshop at Southern University at New Orleans on November 16, and Trusted CI's Damian Rouson also participated in the MS-CC Annual Meeting May 29-31 in Washington, DC.

**Metrics. Table 4** provides details for MS-CC CCoP participation during Y5.

**Table 4.** MS-CC CCoP activities during the reporting period

| Date | Topic | Participants |
|---|---|---|
| October | Ransomware (Jim Basney, Trusted CI) | 31 |
| November | Digital Literacy & Cybersecurity (Katie Kehoe, NCAT) | 29 |
| December | Artificial Intelligence (Anita Nikolich, UIUC) | 32 |
| January | GLBA Cybersecurity Requirements (Dameion Brown, JSU) | 41 |
| February | Regulated Research (Carolyn Ellis, ASU) | 37 |
| March | Penetration Testing - Dameion Brown (JSU), George Bailey (cyberTAP at Purdue) | 41 |
| April | Phishing attacks - Dr. Bharat Rawal (Grambling State University) | 34 |
| May | “A Brief History of Modern AI and why Local AI Matters” - John Fink (Digital Scholarship Librarian at McMaster University) | 41 |
| June | Multi-factor Authentication - Gregory Jones and Mable Moore (Xavier University) | 32 |
| July | Virtual Private Networks - Dameion Brown, JSU | 37 |
| August | CrowdStrike - Open Conversation about Experiences & Lessons Learned - Stephen Bollinger, NCAT | 32 |
| September | Bringing Researchers & IT together for Cybersecurity: Dr. Francis Tuluri (JSU), JSU IT (Dameion Brown, Terry Haygood, Summer Boyd) | 37 |

[20] https://blog.trustedci.org/2023/10/ms-cc-cybersecurity.html

# 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),[21] 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. The document is a living document and updates are made on an ongoing basis.

**Progress this year.** In Q1**,** Trusted CI incorporated OSCRP into the broader Trusted CI Framework program and identified areas for further alignment. One such area was a cybersecurity risk register template, (internally referred to as an "Open Science Cyber Risk Register"), designed to help organizations compile and evaluate their overall cyber risk posture.

In Q2, Trusted CI developed a project plan for the risk register template, identified a timeline, and began development. Trusted CI also discussed risk registers with the RISC during its January 2024 workshop and solicited ideas and feedback.

In Q3, Trusted CI continued its work developing a risk register template and corresponding guidance document.

In Q4, Trusted CI showcased a draft version of the risk register template with the RISC group and solicited feedback. In response to this presentation, several community members requested to begin using the draft template, and agreed to offer feedback to Trusted CI on their experiences.

**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.

## 2.2 Situational Awareness / Cyberinfrastructure (CI) Vulnerabilities

**Background.** In collaboration with Open Science Grid, the NSF supercomputing centers, and the ResearchSOC, Trusted CI managed a situational awareness service that the community could count on for high-quality, easy-to-follow notifications on relevant vulnerabilities and threats. Trusted CI tracked 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; 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 leveraged our relationships with the NSF supercomputing centers (NCSA, PSC, and other ACCESS CI service providers). We filtered issues for those relevant to the

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

community and then supplied simple guidance for mitigating vulnerabilities. Trusted CI utilized its existing email lists and encouraged a dialog with our stakeholders for further discussions and feedback. Notifications are archived and searchable from the Trusted CI email archives.[22,23]

**Progress this year.** Between July 1, 2023 and April 30, 2024, 18 critical vulnerabilities were communicated to the community after evaluating a total of 31.

In April 2024, OmniSOC launched the OmniSOC Community Advisory,[24] a semi-monthly newsletter highlighting current events and information security news aimed at the research cyberinfrastructure community. At the same time, Trusted CI announced the sunsetting of the CI Vulnerabilities mailing list.

**Metrics.** The number of subscribers on the CI Vulnerabilities list was 188 at the end of April 2024 when the list was closed. From the initial formation of CTSC in 2014 to the closure of the CI Vulnerabilities mailing list in 2024, Trusted CI issued nearly 200 alerts to the community.

## 2.3 Ransomware for Data in Motion

**Background.** Trusted CI collaborated with the Polytechnic University of Valencia (Spain) to implement a proof of concept of a ransomware attack on data in motion. This scenario leveraged and was based on the results from analysis on ransomware that Trusted CI conducted in 2023.

**Progress this year.** Implemented a ransomware attack on data in motion in a testbed and used machine learning techniques to detect such an attack happening in real time.

**Metrics.** One paper accepted for publication (see section 2.4).

## 2.4 Publications

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

**Progress this year.** The following were published in Y5:

- Andrew Adams, Dan Arnold, Jeannette Dopheide, Ryan Kiser, Mark Krenz, Drew Paine, Sean Peisert, Michael Simpson, and John Zage, “Trusted CI Operational Technology Procurement Vendor Matrix,” Dec. 14, 2023. DOI: 10.5281/zenodo.10257813
- Raul Reinosa, Clara Valero, Jose Martinez, Elisa Heymann, Ignacio Lacalle, Barton Miller, Carlos Palau, “Empirical Analysis and Practical Assessment of Ransomware Attacks to Data in Motion,” *2024 IEEE International Conference on Cyber Security and Resilience (IEEE CSR),* accepted for publication, September 2024.

[22] https://groups.google.com/a/trustedci.org/g/cv-announce/
[23] https://list.iu.edu/sympa/arc/cv-announce-l/
[24] https://list.iu.edu/sympa/info/omnisoc-community-advisory-l

## 2.5 Training

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

**Progress this year.** Bart Miller and Elisa Heymann taught a tutorial on Secure Programming and Dependency Analysis Tools at the 2023 Internet2 Technology Exchange in Minneapolis in September 2023. Susan Evett, senior manager at Internet2, gave us the following feedback: “Thank you again for teaching that tutorial – it was VERY well received!”.

In July we gave a webinar for Trusted CI on the Ransomware Landscape.

**Image 5.** Miller training at the Internet2 conference.

**Image 6.** Heymann training at the Internet2 conference.

We taught two half-day tutorials on Secure Programming and Dependency Analysis Tools this year:

- 2023 NSF Cybersecurity Summit in Berkeley, California, in October (**Image 7**).
- Supercomputing ’23, in Denver, Colorado, in November 2023.

Both tutorials included hands-on exercises so the attendees could get practical experience with the topics covered.

**Image 7**. Tutorial at the 2023 NSF Cybersecurity Summit


We offered a series of additional training and workshop opportunities at the 2023 NSF Cybersecurity Summit in Berkeley, California, including:

1) The Trusted CI Framework (Scott Russell, Craig Jackson)
2) Security Log Analysis (Mark Krenz, Ishan Abhinit, Phuong Cao)
3) Regulatory Compliance for Research (Anurag Shankar, Will Drake, Tim Daniel, Scott Russell)

We had two tutorials accepted at leading venues on Software Security and Dependency Analysis Tools:

- Supercomputing ’24, for November in Atlanta.
- Internet2 Technology Exchange 2024 for December in Boston.

## 2.6 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, 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. We have also been developing free and open online software assurance training materials.

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 code authorship identification at the 7th NATO Maritime Interdiction Operational Training Center Conference on Cyber Security in Maritime Domain at the NATO Souda Base in Chania, Greece, in September 2023. We are also teaching "Introduction to Software Security" (CS 542) at the University of Wisconsin-Madison (based on UW-Madison instructional funding) using materials developed under Trusted CI. There are two sections with 160 students in total.

We published version 2.0 of the Guide to Securing Scientific Software[25] with a companion blog post.[26] Similarly, we published our report on a technical taxonomy and landscape for ransomware[27] with a companion blog post.[28]

Bart Miller and Elisa Heymann continued producing teaching material, available at https://research.cs.wisc.edu/mist/SoftwareSecurityCourse/. The new material includes four new or updated book chapters:

1. 2.2 Overview of Threat Modeling (updated/expanded)
2. 2.3 Microsoft Security Design Lifecycle and Threat Modeling (new)
3. 2.4 Microsoft DREAD Threat Categories (new)
4. 2.5 PASTA Threat Modeling Methodology (new)

In addition, two new videos were produced by our first outside collaborators. These videos will be linked to our main page.

5. 8.1 Crypto basics (new)
6. 8.2 Crypto tools (new)

We taught "Introduction to Software Security" (CS 542) at the University of Wisconsin-Madison (covered under UW-Madison instructional funding), using materials developed under Trusted CI (Images 4, 5, and 6). For this class we arranged for our students to take part in a ransomware response cyber tabletop exercise (Image 7) facilitated by the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, with support from organizations including the Wisconsin National Guard Cyber Protection Team, FBI Cyber Investigation Team (Milwaukee), and Point Beach Nuclear Plant.

Comments from the CS 542 students:

> "Thanks to this class and you two [Miller and Heymann], I can definitely see myself working in the software security field in the future!"

[25] https://doi.org/10.5281/zenodo.8137009
[26] https://blog.trustedci.org/2023/07/v2-software-guid.html
[27] https://doi.org/10.5281/zenodo.8140464
[28] https://blog.trustedci.org/2023/07/ransomwarereport.html

“Thank you for the great class! This has been my favorite CS course! I've enjoyed the process of learning about and finding vulnerabilities, and then fixing them.”

**Images 8, 9, and 10**. Introduction to Software Security at the University of Wisconsin-Madison

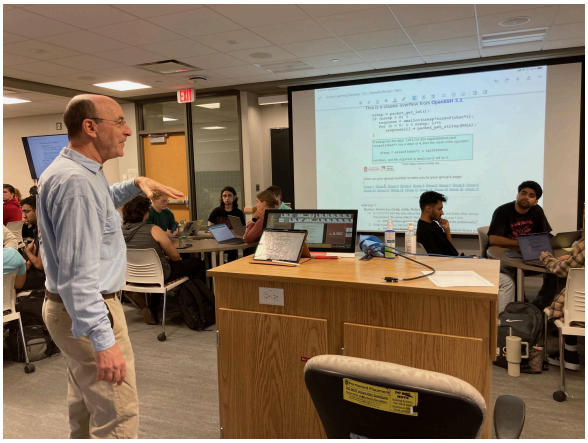


**Image 11**. Tabletop exercise


For free and open online software assurance teaching and training materials, we created 10 new exercises on web security to teach the cross-origin resource sharing (CORS) mechanism (and its limitations). The exercises include attacks using GET, POST, and FETCH methods.

The software on the virtual machine we use for the hands-on exercises was getting outdated, so we updated it with the latest version of the different software packages/systems we need to run our exercises. As a consequence of that we had to do some major rewriting of our WisClick application. WisClick is the web application we use to teach hands-on exercises on web security.

We met periodically with team members to do preliminary work for the Software Assurance Framework (SAF). One of the goals was to understand the parallels and differences between the Trusted CI Framework and the future SAF.

We conducted research on mechanisms for detecting ransomware when affecting data in motion, which is a topic that goes beyond the current state-of-the-art in ransomware.

**Metrics.** 141 students took CS 542 “Introduction to Software Security” course (two sections) at the University of Wisconsin-Madison.

Download statistics for software assurance training materials:

- Text chapters and papers: **45,045**
- Hands-on exercises and instructions (note that our base virtual machine contains almost all the exercises): **8,829**
- Video views: **5,105**

## 2.7 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 program's criteria for renewal. Trusted CI CPEs are distributed in the form of badges, currently issued through Badgr,[29] an open source badge issuing website. Badgr has features that allow recipients to share their badges on social media[30] (LinkedIn, Facebook, etc.).

**Progress this year.** In PY5 we hosted seven webinar events that qualified for CPE badges. We issued 2023 badges to the Trusted CI Fellows. And we issued badges to 2023 Summit attendees.

**Metrics.** The following badges were issued during PY5:

- 207 issued to webinar attendees
- 217 issued to NSF Cybersecurity Summit attendees
- 7 issued to the 2023 Fellows

## 2.8 Project Impact Metrics

**Background.** Trusted CI is charged with addressing cybersecurity challenges affecting NSF projects and facilities. 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 (small and large) and 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 recorded interactions with 17 projects in the last year among the 330 attendees at our webinar, as well as 40 projects among the 321 attendees from the NSF Cybersecurity Summit, with some overlap with the webinars: two projects from the BIO directorate, 27 projects from the CISE directorate, four projects from the EHR directorate, four projects from the ENG directorate, six projects from the GEO directorate, four projects from the MPS directorate, and one project from the OIA directorate, and one project from the TIP directorate. Note that not all event attendees provide NSF project information to us. The following are the projects with recorded Trusted CI interactions this year:

- ACO: An Open CI Ecosystem to Advance Scientific Discovery (OpenCI)
- Category I: Bridges-2: Scalable Converged Computing, Data, and Analytics for Rapidly Evolving Science and Engineering Research
- CC* CIRA: Shared Arkansas Research Plan for Community Cyber Infrastructure (SHARP CCI)

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

- CC* Data Storage: High Volume Data Storage Infrastructure for Scientific Research and Education at Kennesaw State University Shared as Open Science Data Federation Data Origin
- CC* Regional Computing: ORCA: Oregon Regional Computing Accelerator
- CCRI: Planning-C: A Community Research Infrastructure for Integrated AI-Enabled Malware and Network Data Analytics
- Characterization of Chemosensory Pathways in Cnidarians
- CI CoE: CI Compass: An NSF Cyberinfrastructure (CI) Center of Excellence for Navigating the Major Facilities Data Lifecycle
- CICI: Regional: Substrate for Cybersecurity Education; a Platform for Training, Research and Experimentation (SCEPTRE)
- CICI: UCSS: Building a Community of Practice for Supporting Regulated Research
- Collaborative Research: CCRI: NEW: Open Community Platform for Sharing Vehicle Telematics Data for Research and Innovation
- Collaborative Research: EAGER SaTC-EDU: Artificial Intelligence and Cybersecurity: From Research to the Classroom
- Collaborative Research: Frameworks: Sandpiper - A community toolchain to support geomorphology from data acquisition to analysis
- Collaborative Research: SaTC: EDU: Authentic Learning of Machine Learning in Cybersecurity with Portable Hands-on Labware
- Conference: Research Computing at Smaller Institutions (RCSI)
- CyberCorps Scholarship for Service (Renewal): Cybersecurity meets Artificial Intelligence for preparing the Next Generation of Cybersecurity Professionals
- CyberTraining: Pilot: Interdisciplinary Cybersecurity Education to Support Critical Energy and Chemical Infrastructure
- Equipment: MRI: Track 2 Acquisition of a High-Performance Computing Cluster for Boosting Artificial Intelligence Enabled Science, Engineering, and Education in South Carolina
- Excellence in Research: iMed-Sec: Exploring Hardware-Assisted Solutions for Energy-Efficient Low-Overhead Security and Privacy for the Internet-of-Medical-Things
- FMitF: Track II: Bringing Verification-Aware Languages and Federated Authentication to Enable Secure Computing for Scientific Communities
- Frameworks: Software NSCI-Open OnDemand 2.0: Advancing Accessibility and Scalability for Computational Science through Leveraged Software Cyberinfrastructure
- HiSeasNet: Expanding Coverage and Real-Time Data Collection Capabilities for UNOLS Vessels
- I-Corps: Liveness detection and integrity authentication of digital audio
- IRNC Core Improvement: Accelerating Scientific Discovery & Increasing Access - Enhancing & Extending the Pacific Wave Exchange Fabric
- LIGO Laboratory Operations and Maintenance 2019-2023
- Management and Operations of the Gemini Observatory
- Mid-scale RI-2 Consortium: Biogeochemical-Argo: A global robotic network to observe changing ocean chemistry and biology
- Mid-scale RI-2 Consortium: Network for Advanced NMR

- MRI: Acquisition of Autonomous Plug-In Hybrid Vehicle Platform for Multidisciplinary Research and Education at the University of Michigan-Dearborn
- National Radio Astronomy Observatory: Very Large Array Operations and Maintenance
- Natural Hazards Engineering Research Infrastructure: Computational Modeling and Simulation Center 2021-2025
- Natural Hazards Engineering Research Infrastructure: Experimental Facility with Large, Mobile Dynamic Shakers for Field Testing 2021-2025
- Natural Hazards Engineering Research Infrastructure: Natural Hazard and Disaster Reconnaissance (RAPID) Facility 2021-2025
- NSF's National Optical-Infrared Astronomy Research Laboratory (NOIRLab): Management and Operations of Vera C. Rubin Observatory
- Research Infrastructure: CC* Data Storage: Rice Collaborative Object Store
- Research Infrastructure: CC* Regional Networking: The Pennsylvania Science DMZ supporting under resourced colleges and universities (PA Science DMZ)
- Research Infrastructure: Mid-scale RI-1 (M1:IP): SPHERE - Security and Privacy Heterogeneous Environment for Reproducible Experimentation
- RII Track-1: Data Analytics that are Robust and Trusted (DART): From Smart Curation to Socially Aware Decision Making
- SaTC-CCRI: Collaborative Research: Sharing Expertise and Artifacts for Reuse through Cybersecurity CommunityHub (SEARCCH) (SRI International)
- SaTC: CORE: Small: Linking2Source: Security of In-Vehicle Networks via Source Identification
- Ship-based Science Technical Support in the Arctic (STARC)
- Southern Ocean Carbon and Climate Observations and Modeling (SOCCOM2)
- Track 1: ACCESS Resource Allocations Marketplace and Platform Services (RAMPS)
- Track 2: Customized Multi-tier Assistance, Training, and Computational Help (MATCH) for End User ACCESS to CI
- Track 3: COre National Ecosystem for CyberinfrasTructure (CONECT)
- Track 4: Advanced CI Coordination Ecosystem: Monitoring and Measurement Services
- University of Alaska Fairbanks/Sikuliaq Oceanographic Instrumentation (2019)
- University of Alaska Fairbanks/Sikuliaq Oceanographic Instrumentation (2020)
- Virginia Tech CyberScholars Program

**Metrics.** Our updated metrics are captured in **Images 12 and 13**.

**Image 12.** Chart of total NSF directorate impact since 2012

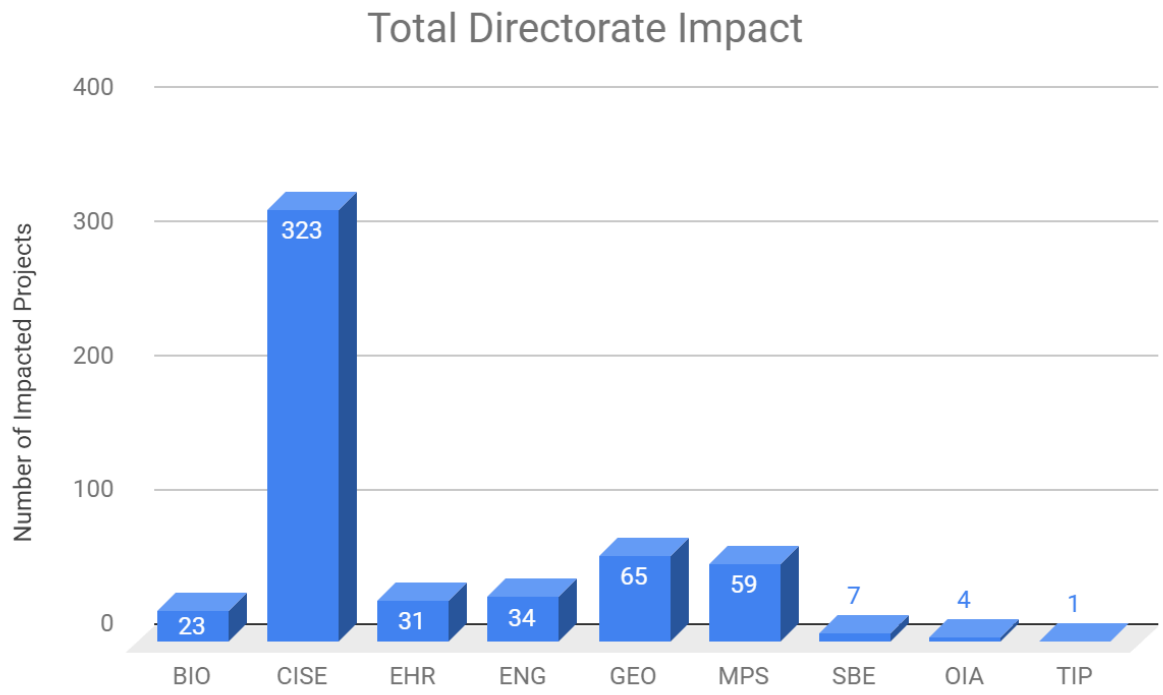
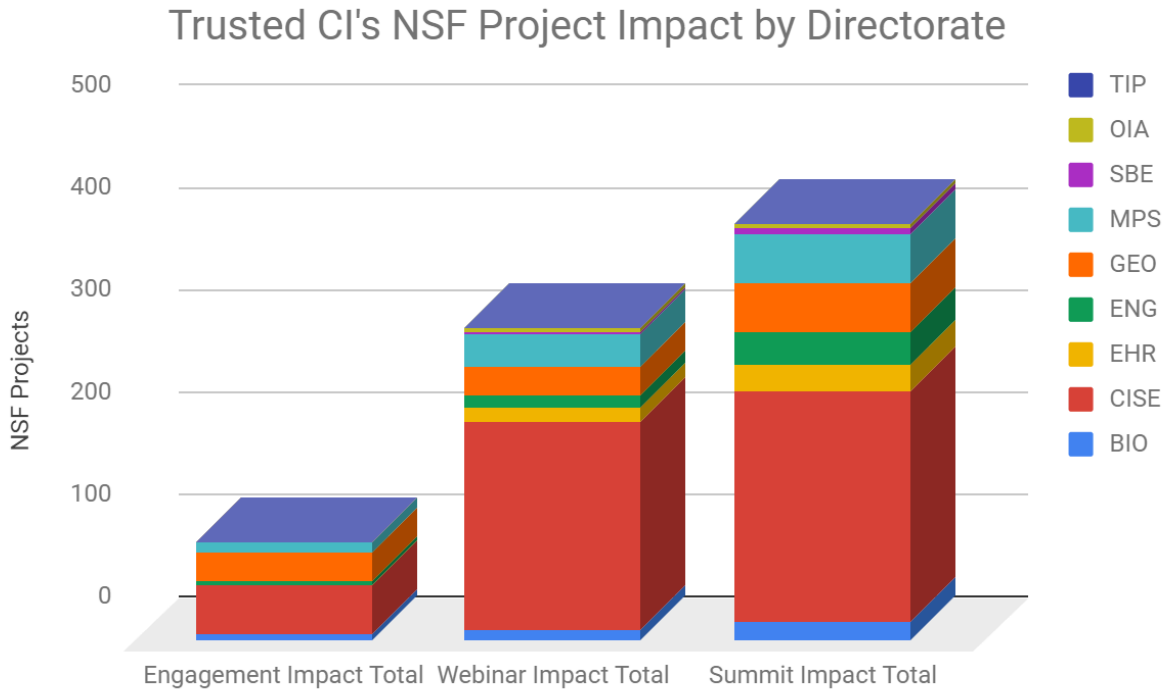



**Image 13.** Chart of NSF project impact by directorate and activity type since 2012



## 2.9 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; refined Trusted CI's RISC; initiated development of an initial cohort reassessment approach; began an assessment of revisions needed to update the FIG; and initiated a number of revisions to the cohort program. We also captured the Framework's broader impacts illuminating from the state of Indiana's Local Government Cybersecurity Assessment Program.

**Trusted CI Framework Cohort:** Trusted CI has graduated five cohorts since inception of the program in 2022. We continue to see impact during cohort sessions. For example, some organizations designated a cybersecurity lead or initiated hiring for that role, and initiated policy development activities. Cohorts Delta and Echo, who completed the engagement during this period of performance, included the following organizations:

| Organization | Type | Cohort |
|---|---|---|
| National Center for Supercomputing Applications (NCSA) | HPC | Delta |
| National Corporation for Atmospheric Research (NCAR) High Performance Computing Division | HPC | Delta |
| Pittsburgh Supercomputing Center (PSC) | HPC | Delta |
| San Diego Supercomputer Center (SDSC) | HPC | Delta |
| Texas Advanced Computing Center (TACC) | HPC | Delta |
| Advanced Simon Observatory (ASO) | Mid-scale R2 | Echo |
| Consortium: Compact X-ray Free-Electron Laser Project (CXFEL) | Mid-scale R2 | Echo |

| Organization | Type | Cohort |
|---|---|---|
| Inter-university Consortium for Political and Social Research (ICPSR) | Mid-scale R2 | Echo |
| National High Magnetic Field Laboratory (MagLab) | Major Facility | Echo |
| Security and Privacy Heterogeneous Environment for Reproducible Experimentation (SPHERE) | Mid-scale R1 | Echo |
| TMT International Observatory LLC (TIO) | Other | Echo |

**Trusted CI Framework RISC:** We are continuing to evolve the RISC initiated by Trusted CI in 2023. This is an important initiative to strengthen our engagement with the NSF community. Specifically, RISC uses the Trusted CI Framework cohort experience as a foundation for ongoing cybersecurity community building among the cohort alumni and facilitating quarterly workshops on a myriad of cybersecurity topics. Trusted CI facilitated four quarterly workshops during this period of performance. Key highlights this year included:

- Welcoming Delta and Echo cohorts to the community.
- Conducting our first two in-person workshops—one each in conjunction with the 2023 NSF Cybersecurity Summit and 2024 NSF Research Infrastructure Workshop.
- Facilitating breakout sessions to aid the development of a cybersecurity risk register, led by Scott Russell.
- Initiating development of a charter to formalize RISC vision and goals.
- Presenting an overview of proposed updates to the cybersecurity section of the NSF's RIG, led by Mike Corn, NSF's Cybersecurity Advisor for Research Infrastructure.

**Framework Reassessment Approach Development:** In 2H2024, the Framework team initiated an activity to develop a Framework reassessment approach for organizations that completed a cohort engagement. This initiative will help organizations measure progress toward Framework implementation and will also be important for assessing Trusted CI impact on these organizations. We are seeking to achieve roughly the same level of confidence in the ratings for reassessments as the original cohort, but much more efficiently. We initiated development of the following major reassessment approach components:

- Develop major design requirements
- Determine the timing and scheduling
- Identify reassessment deliverable(s)
- Develop a CY2025 Project Plan

**FIG Revision Requirements Identification:** The Framework team initiated a complete review of the Trusted CI FIG[31] to identify proposed changes and estimate the level of effort required. The results of the initial reviews show the first revision will be a major update to version 2.0. We anticipate completing the review process before the end of CY2024. Information gathered from the review process will help determine the quantity and complexity of updates needed along with an estimated level of effort. The expected timeframe to begin updates is to be determined.

**Cohort Program Refinements:** The Framework team initiated an activity to refine elements of the cohort program; to enhance its impact and make the process more efficient overall. Developing an assessment scoping process, updating training materials, and completing development of a cohort workflow checklist are among several initiatives in 2H2024. The goal is to complete refinements prior to the start of the next cohort [Foxtrot] in 1H2025.

**Broader Impacts:** The State of Indiana local government cybersecurity assessment program, Cybertrack, prominently features the Trusted CI Framework. The Cybertrack assessment methodology integrates a smaller subset of Trusted CI Framework Musts[32] and CIS controls. In June 2024, the joint Indiana University/Purdue University Cybertrack[33] program released a second local government cybersecurity assessments report that included a much larger population. This report showed entities' total scores on the assessed Framework Musts "**significantly**" predict entities' total technical controls scores.[34] Data from this report is strong evidence that a Framework-aligned cybersecurity program enables solid cybersecurity practices at the operational level.

The Cybertrack methodology gained recognition **nationally over the course of this period of performance. Here are several highlights from this year:**

- Dec. 2023 - Govtech.com published an interview with state of Indiana's Chief Information Officer Tracy Barnes that highlighted Cybertrack.
- Jan. 2024 - Cybertrack was among the topics discussed when Craig Jackson and George Bailey visited the University of Cincinnati-based Ohio Cyber Range Institute. This was a worthwhile meeting leaving the door open for continued engagement.
- Feb. 2024 - Lawfare published an article prominently featuring Cybertrack. Team members Craig Jackson, Emily Adams, and Scott Russell are among co-authors contributing to the article.
- March 2024 - Ann Cleaveland, described our work as a model for what all cybersecurity clinics should be chasing during an IU Center for Applied Cybersecurity Research (CACR) Speaker Series presentation. Ann is a leader in The Consortium for Cybersecurity Clinics and Executive Director of UC Berkeley's Center for Long -Term Cybersecurity(CLTC).

[31] https://doi.org/10.5281/zenodo.4562447.
[32] Ibid.
[33] https://incybertrack.org/.
[34] Cybertrack Report: Aggregate Results & Analysis from 76 Assessments (May 2023 - May 2024), p. 21.

- March 2024 - Craig Jackson presented a talk on the Transformative Twelve and Cybertrack findings at NSF's 2024 Research Infrastructure Workshop.
- June 2024 - Craig Jackson served on a panel at Cyber Civil Defense Summit presented by CLTC. The panel, called "Academia's Role in Cyber Defense" about the Cybertrack program … and lessons learned about how higher-ed programs like Cybertrack can help bolster cyber resilience in local communities."

**Metrics:**

- The Trusted CI Framework is having impact beyond the NSF community.
- The majority of NSF Major Facilities have adopted the Trusted CI Framework.

## 2.10 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 Fellows attended the 2023 Cybersecurity Summit as planned. During the event, a 30-minute panel session with the Fellows was presented, featuring a quick introduction of all seven Fellows. They were recognized for graduating from the program and were presented with Trusted CI plaques bearing their names. The Trusted CI Fellows program has been demonstrably successful over the past five years, but we also recognize that there are many ways in which we can expand the impacts of this program going forward. Given this and the fact that under the current award, we only have a partial calendar year, we did not have a 2024 class of Fellows. Instead, we will have a Fellows reunion event at the NSF Cybersecurity Summit in October 2024. We hope to begin refreshing the curriculum under the Trusted CI renewal award in late 2024. We have 12 former Fellows that will attend the 2024 Cybersecurity Summit. We will be hosting a 60-minute panel session with the alumni Fellows, and Rick Wagner, a previous Fellow, will be moderating the panel. Moving forward, we plan to introduce a new curriculum and will be seeking feedback from the alumni Fellows. Sustainable Horizons Institute (SHI) will be assisting with re-envisioning the Fellows and student programs. With a focus on reaching underserved communities and expanding the value and impact for each program respectively. Initial discussions began at the Trusted CI All Team Meeting held in August with the involvement of Mary Ann Leung, Ph.D of SHI.

## 2.11 Law and Policy Insights

**Background.** IU's 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 a more granular analysis of what those requirements mean and how to approach their implementation.

**Progress this year.** In Q4 and Q1, Trusted CI onboarded one student for the Fall 2023 semester, identified a research topic (cybersecurity insurance controls requirements), and developed an outline. The student then produced a draft memorandum on cybersecurity insurance controls requirements, iterated on feedback, and then finalized their research memorandum.

In Q2, Trusted CI onboarded one student affiliate for the Spring 2024 semester, identified a research topic (cybersecurity requirements for water systems), developed an outline, and produced a draft. Scott Russell presented at the CACR Cybersecurity Conversations on the research of the student affiliate from Fall 2023

In Q3, the student affiliate finalized their research memorandum. Scott Russell presented on the student's research during the July 12 CACR Cybersecurity Conversation. The project also coordinated with the IU Maurer School of Law to identify two students for the Fall 2024 semester.

In Q4, Trusted CI onboarded two new students for the Fall 2024 semester and identified research topics for each (1) the False Claims Act as applied to cybersecurity contractual requirements; and 2) Cybersecurity Supply Chain Risk Management).

## 2.12 Annual Challenges

**Background.** Trusted CI has run Annual Challenges since 2020. In 2020 Trusted CI led a community study on trustworthy data, leading to a public findings and solutions document. In 2021, Trusted CI embarked on a study that sought to broadly improve the robustness of software used in scientific computing with respect to security. It delivered a findings document as well as a *Guide to Secure Software* intended to be a living document maintained by Trusted CI. In 2022, Trusted CI examined the security of operational technology (OT) (or cyber-physical systems) used in science. This led to publications of a findings document[35] and a multi-year roadmap of solutions to advance security of OT used in research facilities.[36]

The 2023/2024 Annual Challenge is engaging with MFs undergoing construction and refreshes in a hands-on way to build security in — particularly with respect to OT — from the outset.[37] Trusted CI is directly supporting the planning for facility refreshes or construction with respect to information and OT. Our focus in 2023/2024 began with "ships and poles" but has since expanded. The engagees tie directly into the Ambassadors program and, in some cases, also 2023/2024 Framework Cohorts. Specifically, in 2023/2024, Trusted CI engaging with the Scripps Institution of Oceanography team designing the California Coastal Research Vessel (CCRV);[38] the team at Oregon State University (OSU) supporting the design and construction of the Research

[35] https://blog.trustedci.org/2022/07/findings-of-2022-trusted-ci-study-on.html
[36] https://blog.trustedci.org/2022/11/publication-of-trusted-ci-roadmap-for.html
[37] https://blog.trustedci.org/2023/01/announcing-2023-trusted-ci-annual.html
[38] https://scripps.ucsd.edu/news/naval-architect-selected-uc-san-diegos-new-california-coastal-hybrid-hydrogen-research-vessel

Class Research Vessels (RCRVs);[39] and OSU and Woods Hole Oceanographic Institution teams refreshing the autonomous underwater vehicle and glider fleet for the Ocean Observatories Initiative (OOI). The CCRV, the world's first hydrogen-hybrid research vessel, along with the three RCRVs, are expected to join the U.S. Academic Research Fleet (ARF). The U.S. Antarctic Program (USAP) teams designing the Antarctic Research Vessel[40] and supporting the refreshes for USAP land facilities (McMurdo, Palmer, and Amundsen-Scott South Pole stations) have also recently been added to this effort and are supporting Trusted CI's insights into the challenges and best practices in this domain.

**Progress this year.** "Ships & Poles," now named "Secure by Design" to reflect our plans to expand into other areas of OT within our community, continues to build on its outreach efforts.

In Q4, OOI was added to Trusted CI's secure-by-design effort. The U.S. Antarctic Program (USAP) teams designing the Antarctic Research Vessel (ARV)[41] and supporting the USAP land facilities refreshes (McMurdo, Palmer, and Amundsen-Scott South Pole stations) were also added to this effort and are 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.

Site visits have took place 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. These visits were described in a blog post.[42] The *Sally Ride* visit resulted in important insights about cybersecurity perspectives of marine technicians.

We also had conversations with stakeholders connected with academic maritime activities, including University-National Oceanographic Laboratory System personnel, marine technicians, scientists who use these facilities (*e.g.*, oceanographers), software developers connected with oceanographic data collection, and additional ARF facilities, such as the National Deep Submergence Facility. 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.During PY5Q1, we accomplished two major milestones when we hosted a panel discussion at the NSF Cybersecurity Summit and published the Operational Technology Procurement Vendor Matrix.[43]

The panel, "Experiences from SIO (CCRV), OSU (RCRVs), OOI, and USAP in Cybersecure-by-Design Maritime and Polar Design and Construction," included Jon Meyer and Ezra Van Everbroek (CCRV), Chris Romsos (RCRV), Craig Risien (OOI), and Tim Howard (USAP/ARV), with Sean moderating. The panel was a lively discussion about the OTs used in the various projects and how to work toward secure-by-design goals in their own design, refresh, construction, procurement, and acceptance testing activities. One topic that brought a great

[39] https://ceoas.oregonstate.edu/regional-class-research-vessel-rcrv
[40] https://future.usap.gov/arv/
[41] https://future.usap.gov/arv/
[42] https://blog.trustedci.org/2023/07/updates-on-trusted-cis-efforts-in.html
[43] https://zenodo.org/doi/10.5281/zenodo.10257812

deal of discussion and anecdotes is how to manage crucial but obsolete software, risk acceptance, and how to work with vendors early in the process.

In December, the team published the Operational Technology Procurement Vendor Matrix and issued a related blog post.[44] The purpose of the document is to assist those in leadership roles during the procurement process. It's meant to help formulate questions for vendors to discuss security controls on devices that will be used for maritime research.

During PY5Q2, we began drafting a guide to using the OT Procurement Vendor Matrix.[45] We received very positive feedback about the vendor Procurement Matrix when it was presented at the CI Compass Workshop in January 2024.

In February 2024 we had a second interview with members of the maritime vendor, Wärtsilä, where we learned of the various security standards they follow and got some feedback on the vendor matrix from their perspective.

We also presented a poster at RIW in March 2024 that won second place in the poster competition, supported RCRV in its efforts to develop a template for safety drills, and continued our conversations with maritime vendors to ensure grounding of our guidance in the realities of commercial industry. Finally, we added CMB-S4 to the list of organizations that we are supporting, while they were in the early stages of developing their security program, though this is on hold for the time being while the broader CMB-S4 project is also on hold. Note that this past quarter, Mikeal Jones joined the Secure by Design team. His ARF experience on the virtual cybersecurity team (OmniSOC) is very valuable. Ryan Kiser departed the Secure by Design team due to personal leave.

In PY5Q3 we began working with RCRV on developing a template for security event drills, as well as assisting with IT/OT standard operating procedures and acceptance testing.

In PY5Q3, the design of the CCRV which Trusted CI contributed to — was approved.[46]

In PY5Q4, we were invited by members of the R/V *Endeavor*[47] to cruise from Rhode Island down to Bermuda. The visit will serve dual purposes: To move the ship to its next scheduled research site and to host an OT security workshop with Trusted CI. In PY5Q4, we also visited the R/V *Sally Ride* (please see §1.3). We also published v2 of the Trusted CI OT Procurement Matrix[45] as well as the companion guide[48]. An additional visit to the R/V *Sally Ride*, in conjunction with NSF and INSURV (ONR) inspections is expected in the next quarter.

**Metrics.** As with the 2021 and 2022 Annual Challenges, for the 2023/2024 Annual Challenge, many of the metrics will also be measured in future years, as they relate to adoption and impact, which takes time. For the 2023/2024 Annual Challenge, we are working with four MFs (OOI, RCRV construction, United States ARF, USAP) in which GEO/OCE is also represented by

[44] https://blog.trustedci.org/2023/12/announcing-publication-of-operational.html
[45] https://doi.org/10.5281/zenodo.13830599
[46] https://scripps.ucsd.edu/news/design-worlds-first-hydrogen-hybrid-research-vessel-approved
[47] https://marineops.gso.uri.edu/
[48] https://doi.org/10.5281/zenodo.13743314

three MFs that Trusted CI is directly supporting while USAP in GEO/OPP is providing valuable research insight. We had been working with a facility expected to be an MREFC in the next few years from MPS/AST until its funding was put on hold. These divisions (GEO/OCE, GEO/OPP, and MPS/AST) also happen to be the largest sponsors of MFs by far, and so while "only" two divisions are covered, they actually represent a significant majority of NSF's total MFs by both quantity, funding amounts, and numbers of end users. Finally, we note that we have met all milestones.

The 2023/2024 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, which has received highly positive feedback from the organizations that Trusted CI is supporting.

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

This section covers our engagements and consultations with NSF projects and supporting organizations to tackle their specific challenges with cybersecurity in the support of NSF science.

## 3.1 Tapis Engagement

**Background.** Trusted CI collaborated with the TACC to assess the security of the Tapis system. The Tapis Framework provides a hosted, unified web-based API for securely managing computational workloads across institutions.

**Progress this year.** We finished the in-depth vulnerability assessment of Tapis. We found four significant vulnerabilities in Tapis, in addition to some bugs. We wrote a vulnerability report for each of the vulnerabilities we found and also wrote the engagement final report, which Tapis approved. These reports became publicly available on July 1, 2024.[49]

Below is a quote from Richard Cardone, senior personnel for Tapis at the TACC, after receiving one of our vulnerability reports, on November 17, 2023:

[49] https://zenodo.org/records/10214772

"You guys caught a whale! The fix will go in as an emergency patch immediately."

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

**Progress this year.**

- Jim Basney and Jen Schopf did a joint Trusted CI + EPOC consultation for CIMUSE[50] about the University of Missouri's plans to host a "Cyber Range."
- Jim Basney discussed export control use cases with Markus Pflaum, the Chair of the Department of Mathematics at the University of Colorado (Boulder) and directed him to https://www.colorado.edu/rc/secure-research-computing-resources for his export control use case(s). He also connected him to Sarah Braun (ISO) and Shelley Knuth (Assistant Vice Chancellor for Research Computing) for support.
- Jim Basney had a consultation with Trisha Kunst Martinez, CNS Director, ICPSR[51] at the University of Michigan on June 17, 2024 on the topic of zero trust for the Research Data Ecosystem (funded by NSF, HHS, and others).
- Craig Jackson was on a panel at the Cyber Civil Defense Summit and discussed (among other things) the Trusted CI Framework and its application to Cybertrack.[52]

# 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
- Establishing program templates, policies, and procedures
- Reporting

[50] https://www.nsf.gov/awardsearch/showAward?AWD_ID=2201505
[51] https://www.icpsr.umich.edu/web/pages/about/rde/ and https://www.nsf.gov/awardsearch/showAward?AWD_ID=1946932
[52] https://incybertrack.org/

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 delivered all scheduled annual and quarterly reports to NSF. We participated in the NSF-led 48-month site visit, receiving an "Excellent" rating from the convened panel. We developed 2024 project plans and established individual team member effort allocation for all Trusted CI projects.

We held monthly meetings with our NSF Program Officer and reviewed spending for the current period of performance, identifying any risks to timely spend down.[53] We submitted a no-cost extension to allow post-September spending for the NSF Cybersecurity Summit (being held in October, *see* section 1.1).

## 4.2 Advisory Committee Changes and Meeting

**Background.** The Trusted CI AC serves to provide Trusted CI with strategic guidance.

**Progress this year.** We met with our Advisory Committee on September 13, 2023, seeking guidance on our upcoming 48-month review. Subsequently, we concluded the service of our AC with tremendous gratitude. Trusted CI leadership is making adjustments to the AC membership as we approach the end of the current award and envision the scope and goals of our work during a potential renewal award.

**Metrics.** N/A

## 4.3 Trusted CI All Team Meeting

**Background.** Each year, we hold the Trusted CI All Team 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.** We made program adjustments for 2024 based on team feedback received at the 2023 meeting. These adjustments included having regular activity hotwashes during our monthly virtual All Team calls to ensure broad, shared situational awareness regarding all Trusted CI activities and to ensure lessons learned are effectively disseminated for application on other activities.

We held the 2024 meeting in August. This year's meeting included Carolyn Ellis and Mary Ann Leung, participants in the renewal proposal, in anticipation of our activities that will begin in FY25. The team gathered at the Big Ten Center in Rosemont for two half days. There were 30 people in attendance, and we welcomed new team members to Trusted CI: Carolyn Ellis, Mary Ann Leung, Cory Gleyze, and Megha Moncy. On the first day, we discussed the State of Trusted CI, the security program, and the next five years, and had an introduction to the Sustainable Horizons Institute. On the second day, we had discussions and breakout groups to talk about

[53] The current award ends on September 30, 2024, with an NCE through December 2024 to enable expenditures for the 2024 Summit only.

opportunities to integrate Regulated Research, the new Residencies program, and revamped Students and Fellows programs.

## 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 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 delivered our 2024 PEP to NSF in January. This PEP covered the remaining period of performance, through December 31, 2024. The only change to the PEP identified this year is an extension of the reporting period being covered via our annual project report (this report). It will now start with July 1, 2023 (instead of the previously reported October 1).

## 4.5 Personnel changes

The following personnel changes occurred during the reporting period:

- Indiana University (CACR) - Ryan Kiser departed the project. We welcomed Megha Moncy and Mikeal Jones (both of OmniSOC) to the team
- Lawrence Berkeley National Laboratory (Berkeley Lab) - Dr. Drew Paine returned to the Berkeley Lab team to support secure-by-design efforts. Dr. Damian Rouson joined the Berkeley Lab team to support diversity, equity, inclusion, and accountability and software assurance efforts.
- Pittsburgh Supercomputing Center - Jim Marsteller transferred from NCSA to PSC in December 2023. This transfer made sense as Jim lives in Pittsburgh, had previously worked at PSC for 20 years, and has many existing collaborative relationships with PSC staff and the PSC Trusted CI team.
- University of Wisconsin - Sai Chaparala and Gia-Minh Nguyen left Trusted CI at the end of December, after finishing the Tapis engagement.
- University of Wisconsin - Amelia Sitzberger worked for Trusted CI from January to May 2024, and worked on the CORS exercises.
- University of Wisconsin - Devaki Kulkarni joined Trusted CI in September 2024 to work in the Parsl engagement.
- University of Illinois (NCSA) - Jim Marsteller transferred from NCSA to PSC in December 2023.

## 4.6 ResearchSOC Collaboration

**Background.** Trusted CI regularly collaborates with the ResearchSOC project,[54] 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

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

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:

- Outreach to MFs via the Ambassadors Program (*see* Section 1.2)
- The Situational Awareness service (*see* Section 2.2)
- Alignment of ResearchSOC security and operational metrics with the Trusted CI Framework (*see* Section 2.7)
- Their information security programs (*see* Section 5.7)
- Outreach: ResearchSOC presents to the NSF community at Trusted CI-hosted events (e.g., NSF Cybersecurity Summit).

Since NSF award #1840034 ended September 2023, ResearchSOC has merged with OmniSOC, and Trusted CI's engagement has continued with the combined organization.

**Progress this year.** We continued our quarterly meetings between Trusted CI and OmniSOC/ResearchSOC leadership to discuss additional opportunities for collaboration and cross-promotion of events. In recent years, our coordination has increased, including sharing the increasing knowledge about the MFs between the projects through Trusted CI's Ambassadors Program and ResearchSOC's project liaisons. As we organized the program for the 2024 NSF Cybersecurity Summit, we encouraged a proposal from ResearchSOC. We transitioned the CI vulnerabilities program (*see* Section 2.2) to OmniSOC, now producing a semi-monthly newsletter, "The OmniSOC Community Advisory."

**Metrics.** Five points of collaboration.

## 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.** During Q4, our effort was split between finishing up implementing the mitigations to assets that received an 'unacceptable' rating based on the CIS control set self-assessment and providing cybersecurity awareness to staff. The latter was done at Trusted CI's all-team-meeting; it covered various policies governing Trusted CI assets, as well as presenting on the current threat landscape. Additional tasks included bolstering our mitigations to our SquareSpace content (via a static snapshot that can be instantiated in short notice within the cloud), and a system to monitor our DNS records for potential unauthorized alterations.

Mandated by our Framework-driven security program, we reviewed all policy documents governing Trusted CI assets and personnel. Of note, the process required more resources than we initially allocated, for it revealed that multiple policies had diverged significantly from our current operational processes; and in accordance with our 'review policy' these significant

modifications further required leadership to review changes proposed by the ISO. Additionally, the security and IT team worked on migrating our DNS management off of Google Domains, as it was purchased by SquareSpace, to Cloudflare -- a solution that Berkley Labs was employing and pleased with.

Another major task the ISO undertook was exploring solutions to expire and retain data within our Google shared drive. We settled on using Google's Vault to provide us with a rich method of data expiration/retention. Vault enables us to set a default of five years for expiration and with the use of labels, allow us to modify the default behavior (e.g., keep forever) providing us with data retention. Policy and procedures were updated to reflect our use of Vault. Finally, in accordance with our security program, the ISO provided cybersecurity awareness training to staff at the All-Team-Meeting this past August. Topics covered include policies that received substantial changes due to our pre-mentioned policy review, as well as concerns in the current threat landscape, e.g., threats and mitigations to multi-factor authentication methods.

# 5 International Travel and Impact

On September 27 and 28, Mike Simpson, Bart Miller and Elisa Heymann attended the "7th NMIOTC Conference on Cyber Security in Maritime Domain," held at the North Atlantic Treaty Organisation (NATO) Maritime Interdiction Operational Training Centre (NMIOTC), Souda Bay, Crete, Greece. Mike Simpson represented Trusted CI as a conference participant. Attending this conference allowed Mike to learn about current and emerging cybersecurity challenges in the maritime domain and efforts to meet and prepare for those challenges by military, academic, and commercial organizations. Mike is actively using this knowledge and the contacts made at the conference to support Trusted CI's efforts to support NSF facilities and projects with maritime connections; specifically the current Annual Challenge engagements with RCRV, CCRV, OOI, and others. Having representation at this conference increased Trusted CI's visibility into the multinational military and commercial sectors represented at the conference. This supports access to possible subject matter expertise and collaboration partners for future activities.