TRUSTED CI

THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

A Vision for Securing NSF's Essential Scientific Cyberinfrastructure — Trusted CI Five-Year Strategic Plan (2024–2029)

Five-year Strategic Plan

August 1, 2023
Working Draft
Distribution: Public

Jim Basney, Kathy Benninger, Bart Miller, Sean Peisert,
Scott Russell, and Kelli Shute

About this Document

This document is a product of Trusted CI, the NSF Cybersecurity Center of Excellence. This document is expected to evolve with subsequent revisions based on community feedback. Please send any comments to jbasney@illinois.edu and sppeisert@lbl.gov.

About Trusted CI

Trusted CI is funded by NSF's Office of Advanced Cyberinfrastructure as the NSF Cybersecurity Center of Excellence (CCoE). For information about Trusted CI, please visit the project website: https://trustedci.org/

Acknowledgments

We thank the Trusted CI Advisory Committee for their guidance on both this document and on Trusted CI's efforts generally: Neil Chue Hong, Damian Clarke, Eric Cross, Ewa Deelman, Anita Nikolich, Melissa Woo, and Michael Zentner.

This document is a product of Trusted CI. Trusted CI is supported by the National Science Foundation under Grant #2241313. For more information about Trusted CI, please visit: http://trustedci.org/. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation or any of the employers of the authors.

Using & Citing this Work

This work is made available under the terms of the Creative Commons Attribution 3.0 Unported License. Please visit the following URL for details: http://creativecommons.org/licenses/by/3.0/deed.en_US

Cite this work using the following information:

Jim Basney, Kathy Benninger, Bart Miller, Sean Peisert, Scott Russell, and Kelli Shute, "A Vision for Securing NSF Essential Scientific Cyberinfrastructure — Trusted CI Five-Year Strategic Plan (2024–2029)," Trusted CI Report, MMMMM 2023. DOI: XXXXXXX

This work is available on the web at the following URL:
https://doi.org/10.5281/zenodo.8193607

Table of Contents

1 About NSF and Trusted CI

The National Science Foundation (NSF), with a budget of $8.8B (FY22), promotes the progress of science; advances national health, prosperity and welfare; and secures national defense. Nearly $2B (FY22) of NSF's budget funds the operation and construction of NSF Major Facilities and Mid-Scales, which in turn host the instrumentation that enables much of the rest of the science that NSF funds. NSF cyberinfrastructure is an engine of scientific research and innovation and underlies much of the science that Major Facilities enable. Key cyberinfrastructure components, including supercomputers, data repositories, sensor arrays, ships, software systems, and telescopes, are essential to scientific productivity, such that cybersecurity incidents can have a major impact on the scientific enterprise. For the cyberinfrastructure operators, implementing effective cybersecurity programs for these unique cyberinfrastructure components is a complex challenge.

Trusted CI, the NSF Cybersecurity Center of Excellence (CCoE), has been working to overcome this challenge for over ten years. Its success has been noted both by the NSF community, with the 2017 and 2019 reports from the NSF Large Facilities Cyberinfrastructure Workshops [NSF17, NSF19] citing it as a model for future NSF centers and the former director of the NSF Office of Advanced Cyberinfrastructure, referring to Trusted CI as "a very innovative model in providing cybersecurity expertise to NSF large projects such as the NSF Facilities and has been extremely successful." [Par18] (34:26), and the 2021 JASON Report on *Cybersecurity at Major Facilities* [JAS21] indicating Trusted CI's demonstrable impact on improving the cybersecurity posture of many NSF Major Facilities.

This document establishes a revised Trusted CI vision for a secure operation of essential cyberinfrastructure that enables NSF's vision of a nation that leads the world in scientific research and innovation. As the NSF CCoE, Trusted CI assumes responsibility for bringing the vision of a secure operation of essential NSF-sponsored cyberinfrastructure to fruition. Hence, following Trusted CI's vision is its mission statement and new five-year strategic plan to fulfill that role.

2 Trusted CI Vision

In light of the new and unprecedented challenges facing NSF research, Trusted CI has refined its vision to be:

> **For the secure and trustworthy operation of the essential cyberinfrastructure that enables NSF's vision of a nation that leads the world in scientific research and innovation.**

Trusted CI's vision requires certain attributes in the key areas of mission, governance, resources, and controls. Each attribute reflects this future vision, rather than the status quo. The following subsections describe these needed attributes.

Trusted CI's new vision represents a stronger recognition that cyberinfrastructure is essential to scientific research and innovation, and that ensuring the secure operation of that essential cyberinfrastructure is Trusted CI's highest priority. Trusted CI has entered a new era of proactive risk assessment and engagement with CI-operating organizations to more effectively address this priority.

This Trusted CI vision is aggressive and, as described subsequently in Trusted CI's mission statement and strategic objectives, will require collaboration between Trusted CI and other members of the community to fully realize.

3 Trusted CI Mission

What does the NSF community need from Trusted CI? Trusted CI has primary responsibility for bringing the Trusted CI Vision of the secure operation of NSF-sponsored cyberinfrastructure to fruition. Hence, its refined mission statement to support its vision:

> **Trusted CI, in partnership with CI-operating organizations and the broader community of CI professionals, implements effective cybersecurity programs for the essential cyberinfrastructure that enables NSF's vision of a nation that leads the world in scientific research and innovation.**

This refined mission statement recognizes that *Trusted CI must do more than provide guidance*. Implementing Trusted CI guidance can be a significant challenge for CI-operating organizations, for reasons including budget constraints, workforce limitations, and unique aspects of different CI components. Trusted CI can provide templates, how-to guides, training, etc., but Trusted CI should also have a role in implementation, both because Trusted CI can act as a workforce multiplier for CI-operating organizations and because Trusted CI staff can carry valuable experiences and lessons learned across organizations.

Our mission is based on *partnership with CI-operating organizations*. Trusted CI can not assume responsibility for an organization's cybersecurity program, can not operate an organization's cybersecurity controls/systems, and can not be an organization's incident response team. However, Trusted CI can partner with CI-operating organizations on implementation of the cybersecurity program, i.e., aligning the program to the organization's mission, establishing effective governance, making appropriate resource allocation decisions (including partnerships with external cybersecurity providers), and establishing effective cybersecurity controls. Trusted CI's *residencies* program, described below, is a new initiative to help achieve this expanded mission.

4 Background

Trusted CI's vision for secure operation of essential cyberinfrastructure exists to support NSF's Vision, the science missions of NSF Major Facilities and other essential cyberinfrastructure operators.

Trusted CI Impacts

Since 2012, Trusted CI, the NSF Cybersecurity Center of Excellence (trustedci.org)[1] has been leading the community by tackling strategic cybersecurity challenges facing NSF CI operators, helping to build an NSF cybersecurity workforce, and motivating the NSF community with regard to addressing the importance of securing NSF cyberinfrastructure.

While many cybersecurity compliance programs exist (e.g. HIPAA, FISMA, NIST 800-171), most NSF research (e.g., astronomy, climate, physics, geology) does not fall under a compliance program. NSF does not prescribe cybersecurity — it is the responsibility of the awardee. NSF's approach allows NSF cyberinfrastructure operators the flexibility to shape their cybersecurity program to best support their science mission. The organizational mission of each Facility translates into different priorities for cybersecurity. Consider the program for a bank and hospital — confidentiality, availability, integrity, resilience, etc. are all prioritized differently. So this is a good thing for NSF facilities. However, NSF's approach requires the motivation and empowerment of the NSF community to address cybersecurity.

Trusted CI has filled this role by explaining cybersecurity's role in trusted science, building and maintaining a workforce, helping cyberinfrastructure operators bootstrap their cybersecurity programs and tackle challenges, addressing strategic cybersecurity challenges affecting the broader NSF research community, and being a community voice on the national stage. Trusted CI team members are all CI and cybersecurity practitioners. No other organization has a comparable understanding of the cybersecurity needs of NSF science and has the trust of the NSF community to be able to motivate, support, and lead cybersecurity for NSF science. Trusted CI's activities have balanced tensions between focused and broad impact, service and leadership, innovation vs. predictability and "teaching to fish" vs. direct aid.

[1] Originally known as the Center for Trustworthy Scientific Cyberinfrastructure (CTSC)

Trusted CI issued the *Trusted CI Vision for an NSF Cybersecurity Ecosystem And Five-year Strategic Plan (2019-2023)* [TCI18b] in early 2018. This plan established four major strategic objectives: (1): Build and Disseminate the Needed Knowledge, (2) Processes to Sustain the Community, (3) Secure Cyberinfrastructure, and (4) Foster the Workforce and Collaborations.

The center's accomplishments and outcomes with regard to these objectives include:

- Development of the *Trusted CI Framework* and *Trusted CI Framework Implementation Guide for Research Cyberinfrastructure Operators (FIG)*.
- Establishment of four *Framework* Adoption Cohorts (to date) including 13 NSF Major Facilities,[2] three NSF Mid-Scales, and six other significant NSF-related cyberinfrastructure operators and related community members.
    - Major Facilities adopting the *Trusted CI Framework* include the U.S. Academic Research Fleet (ARF), the Geodetic Facility for the Advancement of Geoscience (GAGE), the IceCube Neutrino Observatory, the Laser Interferometer Gravitational-Wave Observatory (LIGO), the NSF Leadership-Class Computing Facility (LCCF),[3] the National Center for Atmospheric Research (NCAR), the National Ecological Observatory Network (NEON), the National Optical-Infrared Astronomy Research Laboratory (NOIRLab), the National Radio Astronomy Observatory (NRAO), the National Solar Observatory (NSO), the Ocean Observatories Initiative (OOI), the Seismological Facility for the Advancement of Geoscience (SAGE), and the U.S. Antarctic Program (USAP).
    - NSF's Mid-Scales adopting the *Trusted CI Framework* include FABRIC, the Network for Advanced NMR (NAN), and the Deep Soil Ecotron (DSE).
    - Additional significant NSF-related cyberinfrastructure operators adopting the *Trusted CI Framework* include Advanced Cyberinfrastructure Coordination Ecosystem: Services & Support (ACCESS), the Corporation for Educational Network Initiatives in California (CENIC), the Giant Magellan Telescope (GMT), OmniSOC, the National Center for Supercomputing Applications (NCSA), the Pittsburgh Supercomputing Center (PSC), and the San Diego Supercomputer Center (SDSC).

[2] Including Major Facilities under construction via the NSF Major Research Equipment and Facilities Construction (MREFC) account.

[3] Including the Texas Advanced Computing Center (TACC) more broadly.

- Influenced the *2022 NSF Research Infrastructure Guide (RIG)* [NSF21b], which now includes reference to the *FIG* and closer alignment with the Trusted CI Framework, and has expanded cybersecurity guidance from a single paragraph to a rich section (6.3).

- Building a relationship with the NSF community and establishing trust in Trusted CI's motive and effectiveness in helping the community with their science missions.

- Gained special insights through deep annual foci in specific domains, including trustworthy data, software assurance, operational technology, and "security by design" in Major Facilities, and developed the resulting *Open Science Cyber Risk Profile (OSCRP)*, the *Trusted CI Guide to Securing Software*, and the *Trusted CI Roadmap for Securing Operational Technology*.

- Educating the NSF community on cybersecurity's role in trustworthy and reproducible science.

- Provided direct engagements and consulting to NSF CI operators and organized the Large Facilities Security Team (LFST).

- Impacting over 500 NSF projects through their attendance at the annual NSF Cybersecurity Summit or a Trusted CI training event, or participation in one of over two dozen direct engagements with Trusted CI.

- Trained 35 Trusted CI Fellows throughout the community in the basics of cybersecurity for science since 2019.

- Motivated NSF to fund a now self-sustaining Research Security Operations Center (ResearchSOC).

- Represented the cybersecurity needs of NSF researchers to higher education leadership, the national information security community congressional representatives, and international partners.

- Launching a monthly webinar series on NSF cybersecurity which drew over 2,300 attendees and nine thousand subsequent viewings of recordings since 2016.

- Providing cybersecurity training sessions to hundreds of community members on topics such as identity management, log analysis, and secure coding.

- Issued cybersecurity law and policies guidance on topics including Controlled Unclassified Information, the EU General Data Protection Regulation, the California Consumer Privacy

Act, US Export Control Laws and Regulations, the DoD Cybersecurity Maturity Model Certification, and Artificial Intelligence & Ethics.

- Re-establishing and growing the annual NSF Cybersecurity Summit to well over 100 attendees each year.

The NSF 2022-2026 Strategic Plan

The NSF 2022-2026 Strategic Plan [NSF22] establishes a vision of "A nation that leads the world in science and engineering research and innovation, to the benefit of all, without barriers to participation." Moreover, it establishes this vision with urgency:

> "NSF's role in supporting research and innovation has never been more important, and the opportunities to create lasting benefits are immense. ...the emergence of zoonotic diseases, the impact of environmental change on agriculture and infrastructure, the prevalence of megafires, changes in marine ecosystems and the ubiquity of plastic waste, from mountain tops to ocean depths, underline the importance of scientific understanding for health, prosperity and welfare."

The three pillars upon which NSF has established its vision include both technical and social dimensions: "(1) Advancing the frontiers of global research and innovation; (2) Ensuring accessibility and inclusivity; (3) Being a leader in the S&E enterprise." Notably, in addition to technical aims of new enabling technologies and accelerating data-science, NSF's vision of inclusivity specifically targets global S&E engagement, responsible and ethical research, the changing nature of science, and including the "missing millions" of individuals who have been "historically underserved, marginalized, and adversely affected by persistent poverty and inequality."

Of course, NSF also discusses cyberinfrastructure as well, including the new observation platforms, sensors, communication systems, satellite systems, and more that will be needed to investigate climate science. It also mentions innovation in manufacturing, wireless, biotechnology, quantum science and engineering, and of course, artificial intelligence. Notably, it indicates: "Research infrastructure, from individual laboratories to major research facilities, is at the heart of the scientific endeavor. ... If the U.S. does not lead the world in research infrastructure, it cannot lead the world in science and innovation."

NSF and NSF Cyberinfrastructure

The NSF community is large and diverse, spanning seven science directorates. This community is tightly integrated with higher education institutions and research laboratories that provide administrative homes for projects. The community also collaborates closely with communities from other federal and non-federal agencies, as well as with the international science community.

NSF-funded cyberinfrastructure is vast. The most impactful of the organizations that operate this cyberinfrastructure , by virtue of the volume of science that they enable, include *Major Facilities*, *Mid-Scale Research Infrastructure*, and the many pieces of *software* that are developed with NSF funding and used widely throughout NSF science.

The diversity of these projects' science missions, combined with the complexities of implementing cybersecurity and open science in tandem, creates a serious cybersecurity challenge. There is no off-the-shelf approach to cybersecurity for open science that the NSF community can adopt. Major Facilities struggle to develop their own tailored approaches.

To address this challenge, an approach is needed to manage risks – while providing both flexibility for facility-specific adaptations and access to the necessary knowledge and human resources for implementation.

New Directorates and Centers of Excellence

Since Trusted CI published its previous strategic plan [TCI18b], NSF and NSF cyberinfrastructure have changed in many ways. Undoubtedly the most significant change has been the creation of the new Technology, Innovation and Partnerships (TIP) Directorate charged with "advancing U.S. competitiveness through investments that accelerate the development of key technologies and address pressing societal and economic challenges." Additional changes include the creation of the Mid-Scale Research Infrastructure program, and the creation of Centers of Excellence, including the Cyberinfrastructure Centers of Excellence (CI CoEs), Centers of Research Excellence in Science and Technology Postdoctoral Research Program (CREST-PRP), and the Centers of Research Excellence in Science and Technology (CREST) and HBCU Research Infrastructure for Science and Engineering (HBCU-RISE).

Research Security

In light of the threat of nation state theft of intellectual property, NSF has also expressed a concern in research security, including research cybersecurity. This concern led to a 2019 JASON study, which resulted in a report, "Fundamental Research Security." [JAS19] JASON was also commissioned in a second study on cybersecurity at Major Research Facilities, resulting in a second report, "JASON Report on Facilities Cybersecurity" containing 13 findings and 7 recommendations [JAS21]. (Trusted

CI responded to both[4] of these reports.[5]) It is worth noting that the concerns expressed by NSF and JASON continue to be demonstrable. A critical recent example is the October 29, 2022 cyberattack against the Atacama Large Millimeter/submillimeter Array (ALMA) that halted research at the facility for 48 days. Of course we will never know of any phenomena that may have otherwise been observed during the time that the facility was incapacitated. One of many results of these reports is the creation by NSF of the position of Cybersecurity Advisor for Research Infrastructure within the Office of the Director of NSF.

Changes in NSF Science

Decadal surveys published by the National Academies of Science provide the visions of various scientific domains for how that scientific domain has changed in the past ten years and how it is expected to and should change in the subsequent ten years.

Automation and AI

Recent National Academies of Science Decadal Surveys indicate the way in which automation of scientific experiments is becoming important. Automated experiments, sometimes referred to as "self-driving labs" [MRZ+23], can be particularly useful in automating the use of *operational technology (OT)* in experiments, as such OT have traditionally required significant human manual effort from which to record sensor observations or to control the function of.

In addition, more automation means not just more software but more *bespoke* software. In cybersecurity terms, bespoke software, sometimes built by individuals without traditional software engineering background, can lead to vulnerabilities. More automation also typically means increasing use of AI/ML, which, as we have discovered, carries its own set of vulnerabilities. Finally more automation can mean that problems can be fixed more quickly, although automated processes that are manipulated by attackers could also have a rapid cascading impact on a much larger system without any human intervention in the loop being possible until after the damage is done. Several quotes from decadal services regarding automation and AI include [NAS20, NAS22a]:

> "Automated data are continuously collected…"
> "Leveraging what has come before, researchers are now incorporating artificial intelligence (AI) and the automation of scientific instruments into the research workflow. … these methods [are now used] to design experiments and to automatically control them. … This closed loop iterates and [can] accelerate discovery by orders of magnitude."

[4] https://blog.trustedci.org/2019/12/JASON-2019-Report.html
[5] https://blog.trustedci.org/2022/03/trusted-ci-applauds-jason-report-on.html

> "In materials science … automation and ML cut the time for synthesis and testing from 9 months to 5 days"
> "In particle physics … workflows that implement inference algorithms allow experiments to achieve, for example, a given sensitivity using half the data."
> "In drug discovery … active learning identified 57% of the active compounds by performing 2.5 percent of the possible experiments, compared with 20% identified through a traditional approach…"
> "Biochemistry researchers use robotics and data science to automate high-throughput synthesis and screening"
> "Astronomers are using ML and … controls on telescopes to automate target selection so that observations are optimally informative given the observational constraints and scientific objectives."
> "In climate science … high-resolution local simulation inform lower-resolution global climate models about processes that can be automated, closing the loop of generating computational experiments and informing a global model with them."
>
> Sources:
> [NAS20] NASEM. *A Vision for NSF Earth Sciences 2020-2030: Earth in Time* (2020)
> [NAS22a] NASEM. *Automated Research Workflows for Accelerated Discovery — Closing the Knowledge Discovery Loop* (2022)

Field-Deployed Facilities

Recent National Academies Decadal Surveys also describe greater use of field-deployed, distributed facilities. These facilities have the key characteristic that they may be outside any kind of traditional perimeter of protection that might otherwise exist on a university campus or in a National Laboratory. Quotes describing this change include [NAS12, NAS19a]:

> "The result is … a 'patchwork' of missions and sensors, with little assurance that critical measurements will be continued for the long term or that new capabilities can be infused in a predictable manner."
> "…less instrumentation in the oceans corresponds to missed opportunities"
> "…a global seismic network [is] a worthy goal"
> "…recapitalization of the $80-$100 million instrument fleet [is] a major challenge. Many of the instruments have been in operation for 12-14 years and the base award for SAGE does not include significant funds for recapitalization."

> Sources:
> [NAS12] NASEM. *Earth Science and Applications from Space: A Midterm Assessment of NASA's Implementation of the Decadal Survey* (2012)
> [NAS19a] NASEM. *Management Models for Future Seismological and Geodetic Facilities and Capabilities: Proceedings of a Workshop* (2019)

Operational Technology

As indicated earlier, decadal surveys anticipate greater use of automation and AI in scientific experiments. Specifically, much of this automation involves operational technology — sensors and control systems that perform and observe steps in experiments. Quotes from recent National Academies Decadal Surveys include [NAS15]:

> "Satellites and autonomous sensor systems have revealed a dynamic global ocean system on unprecedented temporal and spatial scales;"
> "Large, powerful, and fast autonomous underwater vehicles (AUVs) are increasingly used in research and exploration."
> "NSF has greatly benefited from… infrastructure and sensors such as Alvin, moorings, current meters, conductivity-temperature-depth and microstructure sensors, bioacoustics, AUVs, Argo development, and gliders."
> "…advanced remotely operated and autonomous platforms are all technologies that have opened new intellectual vistas, enabled new kinds of research, and described new aspects of the ocean."
> "Unmanned aerial vehicles and autonomous underwater vehicles carry sensors to vantage points from above the ocean surface to the deep ocean, even under ice; floats, gliders, and unattended surface platforms extend affordable spatial and temporal coverage of low-power sensors. "
>
> Sources:
> [NAS15] NASEM. *Sea Change: 2015-2025 Decadal Survey of Ocean Sciences* (2015)

Data

Not unexpectedly, NAS Decadal Surveys report larger facilities and much, much more data [NAS21]:

> "New, coordinated advances … are required to unlock the workings of the … universe."
> "A suite of small and medium-scale ground and space-based observational facilities… Ground-based 20-40m optical-infrared telescopes and an IR/O/UV space telescope significantly larger than HST…"
> "A sensitive next-generation radio observatory more powerful than the VLA …"

> "Next-generation CMB telescopes..."
> "...improve the sensitivity of current ground-based gravitational wave detectors..."
> "Strong software ... to numerically interpret the gravitational wave"
>
> Sources:
> [NAS21] NASEM. *Pathways to Discovery in Astronomy and Astrophysics for the 2020s* (2021)

Research Security

The 2019 JASON report [JAS19] indicates ongoing and even increasing concern about research security (foreign influence/attacks):

> "Actions of the Chinese government and its institutions that are not in accord with U.S. values of science ethics have raised concerns about foreign influence in the U.S. academic sector. JASON reviewed ... evidence suggesting that there are problems with respect to research transparency, lack of reciprocity in collaborations and consortia, and reporting of commitments and potential conflicts of interest..."
> "...academic leadership, faculty, and front-line government agencies lack a common understanding of foreign influence in U.S. fundamental research, the possible risks derived from it, and the possible detrimental effects of restrictions on it that might be enacted in response."
> "Are there areas of fundamental research that should be more controlled rather than openly available?"
> "JASON assesses that a powerful countermeasure against foreign influence would be the careful consideration of foreign engagements by stakeholders before they are initiated. This could be facilitated by a set of assessment tools in the form of a series of questions, tailored to the level of the stakeholder in question."
>
> Sources:
> [JAS19] JASON. *Fundamental Research Security*, December 2019.

Skilled Staffing and Guidance

A macro trend is the increasing difficulty for the academic and public sector to hire skilled cybersecurity staffing in comparison to the private sector. In the case of Silicon Valley technology companies, total compensation for skilled technology workers can easily be 3-5x higher than academic sector salaries, and in some cases, much, much higher. Given that NSF Major Facilities are often run by universities or university coalitions, this effect transfers to Major Facilities as well. Moreover, even if universities were able to significantly increase IT salaries, this would not necessarily solve the problem on its own. Major Facilities generally have fixed budgets but are subject to increasingly higher costs due to inflation. Their ability to pay for IT staffing is consequently lower, as is their desire to pay for such staffing, since Major Facility budgets are zero sum and so an increase in IT budgets would reduce the budget for other aspects of the Facility's scientific mission. Finally, for the Major Facilities who can afford IT cybersecurity staffing, despite the availability of materials such as the *Trusted CI Framework* [TCI18a] and the *Trusted CI Guide to Secure Software* [TCI21c], there is still insufficient cybersecurity documentation and training materials appropriate to the needs and expertise of Major Facilities that remaining security staff can properly leverage and implement.

Threat Landscape

NSF-sponsored cyberinfrastructure has always been a theoretical target, although from the Cuckoo's Egg incident to Stakkato to a wide variety of attacks against NASA, NOAA, and Johns Hopkins Applied Physics Lab facilities,[6] the 2017 attack against the University Western Australia's Zadko Telescope, and the 2018 attack against the Sunspot Solar Observatory in New Mexico, cyberattacks have also been clear and present.

Moreover, as indicated in the JASON reports [JAS19,JAS21] and NSF Research Security notices [NSF23], cybersecurity threats faced by NSF science include — now more than ever — nation state threats aimed at the theft of intellectual property.

In addition, as we have seen, numerous attacks have manifested against scientific facilities in very recent years, notably via ransomware. This includes, but is not limited to:

- 2020 ransomware attack against the Michigan State University Physics and Astronomy Department
- 2020 ransomware attack against the University of California, San Francisco
- 2021 ransomware attack against UK Research and Innovation (UKRI)
- 2021 malware attack against European HPC clusters
- 2022 cyberattack against the ALMA Observatory that forced a 48-day shutdown

Thus Trusted CI takes the perspective that NSF-sponsored cyberinfrastructure remains vulnerable to attack, including by nation state actors, and sees supporting the protection of that infrastructure against such attacks squarely within its mission.

[6] Arun Viswanathan and Jeremy Pecharich. *The New Space Race: Cyber Security for Space Missions*. Jet Propulsion Laboratory Cyber Defense Engineering and Research Group. Oct 11, 2016. https://web.archive.org/web/20210322152321/https://trs.jpl.nasa.gov/bitstream/handle/2014/47148/CL%2316-4773.pdf?sequence=1&isAllowed=y

5 Trusted CI Strategic Plan

Defining Success

A key question that Trusted CI asks itself is: what does the success of Trusted CI look like to NSF and the NSF community? Since the publication of the *Trusted CI Framework*, Trusted CI's answer to this question is adoption of the *Framework* by NSF essential cyberinfrastructure operators, as demonstrated by those operators implementing the *Framework* "Musts," and as evaluated through regular baseline cybersecurity assessments. Of particular interest in demonstrating success is adoption of the *Framework* by the NSF Major Facilities.

But the essential cyberinfrastructure extends beyond the Major Facilities. Success means expanding *Framework* adoption also by NSF Mid-Scale Research Infrastructure and other essential cyberinfrastructure (e.g., essential software providers, ACCESS and the NSF HPC centers).

In our progress to-date, we have conducted three cohorts with baseline cybersecurity assessments of the following Facilities, and have scheduled a fourth, as detailed in Section 4 ("Trusted CI Impacts").

Meeting The Challenge

How will Trusted CI succeed in its revised vision? Trusted CI performs many activities that — demonstrably — work. As such, it should keep doing what works, but should seek to do some things even better.

Standardized procedures can be reflected in the broad and consistent use of instruments such as checklists. Examples of such instruments include the *Trusted CI Framework* and the *Trusted CI Guide to Securing Software* [TCI21c]. There are many reasons why standardized procedures are not adopted by individuals or organizations. As described by Roger E. Bohn, in the context of aviation safety,[7] medicine,[8] and manufacturing,[9] *craft*-based disciplines have historically taken decades to evolve into *evidence-based, standardized practices*. There are many reasons for this, virtually all well-intentioned by those initially reluctant to adopt standardized procedures, but ultimately detrimental. This resistance

[7] Roger E Bohn. *Not flying by the book: Slow adoption of checklists and procedures in WW2 aviation*. 2013. http://wp.me/pycE8-bw

[8] Anita L Tucker, Sarah Zheng, John W Gardner, and Roger E Bohn. When do workarounds help or hurt patient outcomes? The moderating role of operational failures. Journal of Operations Management, 66(1-2):67–90, 2020. https://doi.org/10.1002/joom.1015

[9] Roger E. Bohn. From Art to Science in Manufacturing: The Evolution of Technological Knowledge. Foundations and Trends® in Technology, Information and Operations Management, 1(2):1–82, 2005. https://doi.org/10.1561/0200000002

can ultimately be overcome through attrition and eventual pressure of being an outlier in the face of newcomers who have been brought up through standardized procedures.

In the interim, accelerating adoption of standardized procedures takes patience. It requires well written and coherent checklists and procedures. It requires understanding individual issues surrounding resistance to adopt standard procedures. It requires cataloging and understanding *near-misses* to improve initial sets of standardized procedures that can also ultimately counter resistance. It requires active engagement of leadership (e.g., Principal Investigators, Executive Directors), including not just issuing edicts, but engaging deeply and participating throughout the implementation.[10] Ultimately, new knowledge is acquired, new methods and concepts are introduced, and better performance is achieved. There can be roadbumps when new situations arise, such as new regulations, new technology, or, in the case of NSF, new science that needs to be done. For those situations, there may be a justifiable tendency to fall back to *craft*. As a result, standardized procedures are undoubtedly a continuous process. Therefore, institutional *programs* to implement standardized procedures — such as cybersecurity programs leveraging the *Trusted CI Framework* — that are in turn facilitated and led by organizations such as *Trusted CI*, who can monitor near misses, observe changes in science and technology, and evolve standardized procedures as new information is acquired, can enable the continuous application of standardized procedures to maximal positive effect.

Trusted CI will continue to work with high-impact NSF cyberinfrastructure operators to adopt and implement the *Trusted CI Framework* and surrounding documentation, and encourage NSF essential cyberinfrastructure operators to leverage Trusted CI communities of practice and staff. Facilities and projects need enforceable guidance that is also tractable. We will seek to address the gap between what NSF cyberinfrastructure operators are currently doing with cybersecurity programs and what additional measures they might be willing to accept. Related to this, we will seek to address the absence of adequate budgets for cybersecurity. We will continue to build the *Framework* Community of Practice into a proven-valuable, empowered group of cybersecurity stakeholders. We will also seek to bring more mid-scales into the *Framework* Community of Practice, in addition to those who have joined the cohorts thus far. Critically, we will measure the longitudinal change in cybersecurity programs for whom Trusted CI conducts baseline assessments.

At the same time, to achieve our new vision, Trusted CI needs to move beyond a consulting model. While webinars, engagements, and hands-on training can appear initially successful, it can be hard to determine the long-term results of such efforts. Moreover, what happens when individuals leave a cyberinfrastructure operator, as they always do, or when a project's funding ceases? At Major Facilities,

[10] Steve Lipner and Michael Howard. Inside the Windows Security Push: A Twenty-Year Retrospective. IEEE Security & Privacy, 21(2):24–31, 2023. https://doi.org/10.1109/MSEC.2022.3228098

funding and personnel may well be extremely stable for decades at a time. But at smaller cyberinfrastructure operators even including mid-scales, things are less clear. Perhaps there is a "long tail" to training and when funding ends for one project, personnel will join another, and their individual insights through training translates and follows them. However, we still lack concrete insights about long-term outcomes.

We need to work with the facilities to implement our revised vision and definition of success. *Our vision takes Trusted CI to the "next level," where it can continue its efforts on training, reports, evaluations of practices, and produce other guidance, but would also be able to allocate additional resources to help essential cyberinfrastructure operators implement that guidance.* Specifically, Trusted CI has historically offered webinars, half-day training workshops and six-month engagements. Six months may be sufficient for discovery but often may not be sufficient for ensuring that change is properly implemented. Notably, one-to-one engagements is one model, but not not the only possible approach.

Residencies

Realizing this expanded vision requires a new approach of working more closely with the facilities on security program implementation, which we call "residencies". These residencies could certainly be effective for any of Trusted CI's typical cyberinfrastructure operator constituencies, as well as software projects. In this new model, Trusted CI staff embed themselves for several days at a time with Major Facilities in order to perform more actual hands-on work with Major Facilities: meeting with leadership and other teams, reviewing and editing policies, going over source code with its actual authors, reviewing and editing configuration files, looking at actual physical network topology, and so on. Such residencies could also certainly not just be one-time but could be ongoing deep engagements that monitor and sustain improvements over time. (Note that "residencies" are not intended to take on actual "virtual CISO" or operational cybersecurity roles.)

Cohorts and Communities of Practice

In addition, the *Framework* Cohort has established the value of sustained engagement over multiple years rather than "drive-by" recommendations. It has brought facilities together, structured around the *Framework*, and facilitated by Trusted CI to achieve collective, *sustained* success. Thus, Trusted CI will continue to run *Framework* Cohorts and Communities of Practice but also add additional cohorts and Communities of Practice. Very likely, additional cohorts will include *software assurance* and *operational technology*.

Trusted CI's examination of software used in science exposed weaknesses in the software base common to scientific research [TCI21b]. Software developed for science remains vulnerable. Trusted CI should continue to look for ways to support scientific software developers. A *software cohort* might well have been successful for a number of our past software engagements, and particularly for ones that are not small enough to truly enact meaningful changes on their own following a standard six-monthTrusted CI engagements. Developers of essential NSF software cyberinfrastructure must be engaged to to support the hardening — assurance — of commonly used software elements for the: full software lifecycle. To achieve this, a *Trusted CI Software Framework*, derived from existing Trusted Ci trainings and the *Software Guide* [TCI21c]would need to be developed, at which point, software cohorts can commence.

Similarly, an operational technology (OT) cohort, structured around an OT-centric *Trusted CI Framework* addendum of some kind, containing a corresponding, assessable maturity model, and derived from the 2022 *Roadmap for Securing Operational Technology in NSF Scientific Research* would likely be valuable and similarly effective.

In addition, more generally, the community has benefitted from the risk modeling provided through the *Open Science Cyber Risk Profile (OSCRP)* and Trusted CI's Annual Challenges. Going forward, cyberinfrastructure operators could benefit from a second, more hands-on step in risk modeling as provided through cohorts, communities of practice, and residencies.

Regional Summits

With the NSF Cybersecurity Summit, Trusted CI has had demonstrable success in bringing the cyberinfrastructure operator community together, disseminating knowledge via talks and trainings, and supporting and educating students and Trusted CI Fellows. At the same time, smaller organizations with fewer resources and fewer traditional ties to large-scale cyberinfrastructure operation are less likely to be able to attend or even know the annual NSF Cybersecurity Summit. This creates a *diversity* issue in which potential staff of essential cyberinfrastructure operators of the future are not adequately brought into the fold.

For this reason, Trusted CI should instantiate and investigate the creation of regional NSF Cybersecurity Summits located in areas in which there is a critical mass of potential attendees that are underrepresented in attendance to the annual Summit. The creation of regional summits should be focused on *developing the future workforces of current and future essential cyberinfrastructure operators*. Regional summits should not dilute Trusted CI's focus on large-scale essential cyberinfrastructure operators to smaller scale cyberinfrastructure except insofar as the current staff of smaller cyberinfrastructure operations might eventually move on to become future staff of essential cyberinfrastructure operations — the future personnel of NOIRlab, the U.S. Antarctic Program, or the U.S. Academic Research Fleet, for example.

Regional summits, by their nature, should instill a cognitive comfort level for potential participants not typically used to traveling and attending national meetings. In addition, the location of the regional summits should ideally not require air travel for participants and therefore be more affordable.

Security By Design

Operational security workload is challenging for NSF cyberinfrastructure operators in part due to the lack of *security by design* at the outset as well as the diversity of individual resources. Secure by design is a notion that has been an aim of portions of the computing community focusing on the development of high assurance systems since at least the 1970s, beginning with Salzer and Schroeder's seminal principles of secure design.[11] In parallel with the 2002 *Gates Memo*,[12] Howard, Lipner, and others[13] developed and implemented the Microsoft Security Development Lifecycle[14,15] with the aim of secure-by-design more broadly within Microsoft software development.[16] The SDL was later shared and adopted widely by other software developers. While far from a panacea, the Gates Memo and the SDL eventually rescued Microsoft software, over time, from the rampant scourge of the worms released in the mid-2000s that had largely targeted Microsoft software. In today's software and hardware industries, application of secure-by-design principles by software vendors remains hit-or-miss at best. At the same time, as pointed out by CISA, the alternative is *vulnerable by design*.[17]

With a few albeit important exceptions, surrounding the development of bespoke scientific equipment, for which resource such as Trusted CI's Guide to Securing Scientific Software [TCI21a] and equivalent resources for hardware development should be rigorously applied, NSF cyberinfrastructure operators may have little direct control over the security of the components that they deploy. However, indirect control can be applied in at least two ways: via the security specifications that are provided to vendors prior to acquisition of components, and via the ways in which components are composed and integrated.

Thus, Trusted CI will help mitigate vulnerable-by-design risk factors by focusing on more building security into facilities by design at the outset of construction and acquisition, as it is doing now in its

[11] Jerome H. Saltzer and Michael D. Schroeder. The Protection of Information in Computer Systems. *Proceedings of the IEEE*, 63(9):1278–1308, 1975. https://doi.org/10.1109/PROC.1975.9939

[12] Bill Gates. Memo From Bill Gates, January 11, 2002. https://news.microsoft.com/2012/01/11/memo-from-bill-gates/

[13] Frank Swiderski and Window Snyder. *Threat Modeling.* Microsoft Press, 2004.

[14] Michael Howard and Steve Lipner. Inside the Windows Security Push. *IEEE Security & Privacy*, 1(1):57–61, Jan/Feb 2003. https://doi.org/10.1109/MSECP.2003.1176996

[15] Michael Howard and Steve Lipner. *The Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software*. Microsoft Press. June 2006.

[16] Microsoft Security Development Lifecycle (SDL). https://www.microsoft.com/en-us/securityengineering/sdl/

[17] Cybersecurity and Infrastructure Security Agency, Shifting the Balance of Cybersecurity Risk:
Principles and Approaches for Security-by-Design and -Default, April 13, 2023
https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf

2023 Annual Challenge with NSF academic maritime and polar facilities. Trusted CI will seek to broaden community awareness of the criticality of *secure by design* principles through a major strategic push to more essential cybersecurity operators in pre-operational periods, such as Major Facilities under construction via the NSF Major Research Equipment and Facilities Construction (MREFC) account.

Trusted CI's secure-by-design push for cyberinfrastructure operators will include the underlying security of software and hardware components, communications, as well as physical security. Mitigations will be guided by operational and scientific needs, physical constraints and limitations, environmental conditions, and human usability factors, among other elements.

In terms of the security of individual components, Trusted CI efforts will include working with cyberinfrastructure operators to understand *what* security properties to specify to vendors and *how* to specify those security properties when issuing procurement specifications. In rare cases, where the cyberinfrastructure operator is a sufficiently large procurer of a particular component to actually influence design, the specifications may be provided to vendors that can design directly to them [TCI22a]. More commonly, the security specifications will simply narrow the list of suppliers to those that can adhere to those specifications.

At the same time, there may still be many situations in which no vendor can adhere to the specifications [TCI22a]. For those reasons, as with much of legacy OT, security-by-design must be handled on a system level rather than a component level. Thus, Trusted CI's push will also include architectural discussions that take into account communications and network architecture, required interactions between components (e.g., sonar readings being used for both ship operations and research), and even physical security elements, such as when physical security is assumed by the designer of computing equipment, only later to learn that physical security is impossible due to facility safety requirements, or environmental conditions such as water, high radiation, or extreme temperatures.

Related to all of these activities will be including encouraging and supporting hardware and software standardization across and within Major Facilities, where appropriate, for example, with the three — perhaps just the *first* three — Research Class Research Vessels

Communicating with Leadership

Major Facilities enable the performance of groundbreaking science. At the same time, most do not prioritize cybersecurity. Are they making a rational decision? The reality is that Major Facilities all look like large awards but they really are not. Costs for acquiring physical infrastructure, paying heating, cooling, diesel fuel, food, building maintenance, and so on — are all massive costs. Moreover, Major Facilities are starved for experienced staffing in many technical categories. They cannot afford it, given no room in the bottom line, and they cannot hire, because they do not pay sufficiently enticing salaries. Major facilities *can* hire *some* IT people who are inspired by the scientific mission or exotic geographic aspects (oceans, Antarctic, Chilean mountaintops), but who likely need considerable training to be effective.

These reasons partially underlie the need to expand Trusted CI, in order to provide more in-depth expertise and support for these organizations that cannot hire effectively themselves.

Beyond this, Trusted CI sees a variety of other opportunities as well. For example, it may be the case that the needs of reluctant organizations are not met by current resources. In such situations, as it has done with software security and operational technology, Trusted CI can continue to take an approach of understanding challenges and landscape and write guides, as it has done with software security and operational technology security in the past two years. However, Trusted CI also now sees opportunities to extend this support via form new cohorts to starting to work more in depth on the probworking problems, as well as taking on "residencies." The major changes in Trusted CI's approach are *implementation* and *workforce development*. First Trusted CI will help facilities the *Framework*. Then, Trusted CI will help major facilities staff their cybersecurity program.

Additionally, Trusted CI's traditional audience has included technical personnel involved in cyberinfrastructure operators and cyberinfrastructure producers (e.g., software) However, Trusted CI could potentially focus more on NSF PIs themselves. Trusted CI could also target campus research IT personnel more, for example, via its Fellows program, as campus research IT may be disconnected from our other activities.

Alternatively, perhaps organizations that cannot (or will not) dedicate people to adequately support cybersecurity could be convinced by demonstration of impact via their peers that do commit such resources.

General Approach

Using all of these mechanisms, our ongoing approach is to: 1) identify essential cyberinfrastructure (emerging, evolving), 2) identify the major risks to that cyberinfrastructure, and 3) engage with the CI operators to implement effective cybersecurity programs to address those risks. The complexity, diversity, and size of this essential infrastructure, the staffing challenges at the CI operators, etc., creates a need for expanding the capacity of the Trusted CI team, so that our impact is comprehensive and sustained.

Diversity and Workforce Development

To achieve its new vision, Trusted CI needs to expand the capacity, expertise, and diversity of the team. We note that such expansion should most definitely democratize computing via underrepresented communities to include *the missing millions* [NSF21a]. However, the successes of the first three *Trusted CI Framework* Adoption Cohorts in 2022 and 2023 have shown that the *cohort* model can have both efficiency benefits as well — a relatively small number of Trusted CI staff can facilitate a cohort of numerous cyberinfrastructure operators at once. However, each cohort and community of practice still does require Trusted CI staffing. As such, Trusted CI will seek both to meet the needs of the community as well as seek to deploy the cohort model more broadly across other Trusted CI activities.

Despite the difficulty of cybersecurity staffing, Trusted CI should work to support *diverse* workforce development for *both* NSF CI operators *and* also for Trusted CI. We emphasize that while developing the workforce for both CI operators and Trusted CI are important, cybersecurity staffing for Trusted CI is more sustainable than for NSF CI operators. The reason for this is that the institutions that compose Trusted CI already have *cybersecurity teams*, not a lone "cybersecurity person" for a facility. Trusted CI institutions can hire junior (and inexpensive) cybersecurity personnel into our existing, experienced teams, and then train the junior hires. The critical mass of experienced and junior personnel across the Trusted CI institutions can then back each other up.

In view of the increasing Federal conversation surrounding research security, Trusted CI should also look to expand its institutional partnership to include additional specialization in CMMC type compliance beyond what already exists within Trusted CI institutions.

Strategic Risks

There exist strategic risks to Trusted CI's ability to achieve its revised vision. The most notable of these include the following:

1. Major expansions of Federal cyber security regulations / CMMC to broader categories of research would impose requirements that cyberinfrastructure operators are unfamiliar with. To this end, Trusted CI will include regulated research as a first class activity to facilitate understanding and implementation of such requirements where necessary.
2. Federal initiatives on research security to mitigate foreign theft of IP could monopolize resources that could otherwise be allocated to cybersecurity programs. In anticipation of issues associated with research security, Trusted CI will increase its focus on addressing insider threats in its cybersecurity program development activities.

3. There remains a limited workforce to do the cybersecurity work necessary. Our new and existing Cohorts and Communities of Practice, our new regional summits, and our new program on residencies are designed to amplify the ability of limited staff to meet these challenges. In addition, we will seek to expand the current workforce wherever possible through inclusion of more students, more fellows, and a focus on diversity.
4. In order to maintain its full trust within the community, Trusted CI needs to be seen as independent of the National Science Foundation in specific, given NSF's role as a funder and *de facto* regulator. A model, akin to the Aviation Safety Reporting System (ASRS) on "near misses" is a mitigation to this risk. ASRS reports are not sent to the Federal Aviation Administration (FAA), the regulator. ASRS is instead operated by the National Aeronautics and Space Administration (NASA), which is considered to be an independent and respected scientific agency.[18]

Activities

Trusted CI's strategic activities for the next five years are focused around the four pillars in the *Trusted CI Framework*.

Mission Alignment

Under the heading of *Mission*, Trusted CI seeks to address the topics of Mission Focus, Stakeholders and Obligations, Information Assets, and Asset Classification.

1. Mission Focus: Organizations must tailor their cybersecurity program to the organization's mission.
2. Stakeholders & Obligations: Organizations must identify and account for cybersecurity stakeholders and obligations.
3. Information Assets: Organizations must establish and maintain documentation of information assets.
4. Asset Classification: Organizations must establish and implement a structure for classifying information assets as they relate to the organization's mission.

Trusted CI aims to address Must 1 through continued efforts surrounding Trusted CI's training programs and Communities of Practice. Notably Trusted CI will expand its Communities of Practice to additional communities (discussed further below under *Resources*).

[18] Adam Shostack and Mary Ellen Zurko. Secure Development Tools and Techniques Need More Research That Will Increase Their Impact and Effectiveness in Practice. *Communications of the ACM*, 63(5):39–41, 2020. https://doi.org/10.1145/3386908

Trusted CI's "Law and Policy Insights" effort forms the basis for a core aspect of addressing Must 2. Going forward, Trusted CI's focus on Must 2 will expand to include increased engagement with NSF Program Officers in additional scientific divisions to learn about science challenges from NSF and also to emphasize the importance of cybersecurity in a way that facilitates conversation and understanding between NSF Program Officers and NSF PIs. This increased engagement will also certainly include collaboration with the new Cybersecurity Advisor being hired within NSF.[19]

Additionally, Trusted CI will begin a new focus on regulated research and compliance activities. This effort will build both upon Trusted CI's existing efforts in regulated research[20] as well as the Regulated Research Community of Practice (RRCoP) effort recently funded by NSF.[21]

Asset inventory is a huge challenge and gap for most NSF cyberinfrastructure operators. For Must 3, Trusted CI will begin a new effort developing both training and tools to help NSF cyberinfrastructure operators with their asset inventories. For Must 4, Trusted CI will continue its efforts in characterizing the landscape of cyberinfrastructure being leveraged by NSF cyberinfrastructure operators.

Governance

Under the heading of *Governance*, Trusted CI seeks to address the topics of Leadership, Risk Acceptance, Cybersecurity Lead, Comprehensive Application, Policy, and Evaluation and Refinement.

5. Leadership: Organizations must involve leadership in cybersecurity decision making.
6. Risk Acceptance: Organizations must formalize roles and responsibilities for cybersecurity risk acceptance.
7. Cybersecurity Lead: Organizations must establish a lead role with responsibility to advise and provide services to the organization on cybersecurity matters.
8. Comprehensive Application: Organizations must ensure the cybersecurity program extends to all entities with access to or authority over information assets.
9. Policy: Organizations must develop, adopt, explain, follow, enforce, and revise cybersecurity policies.
10. Evaluation & Refinement: Organizations must evaluate and refine their cybersecurity programs.

There are significant gaps that most NSF cyberinfrastructure operators face in the understanding of facility leadership (e.g., the PI or Executive Director) in the role of, importance of, and resources required to ensure robust cybersecurity in support the scientific mission of each facility. To this end, to address Must 5, Trusted CI will begin new efforts in direct outreach by Trusted CI to campus CIOs,

[19] Cybersecurity Advisor for Research Infrastructure: https://new.nsf.gov/careers/openings/od/od/od-2022-87834
[20] SecureMyResearch: https://cacr.iu.edu/projects/SecureMyResearch/
[21] Regulated Research Community of Practice (RRCoP): https://www.regulatedresearch.org/

NSF PIs, Major Facility directors, NSF Program Officers, and university executives (deans and chancellors/vice chancellors). Trusted CI will also begin new efforts in training for CISOs on how to communicate “up” to leadership. In a related effort, Trusted CI will begin new efforts generally in leadership training for CISOs.

With regard to Must 6, Trusted CI will continue its efforts to maintain and expand the *Open Science Cyber Risk Profile (OSCRP).*

Trusted CI’s efforts surrounding Must 8 will involve continuing efforts in supporting self-assessments by NSF cyberinfrastructure operators, as well as continuing and expanding efforts in Communities of Practice. Finally, Trusted CI’s own Cybersecurity Program represents a form of “Comprehensive Application” by enabling Trusted CI to practice its own advice on itself.

Trusted CI will continue its support of Must 9 through the maintenance and development of templates for use in *Trusted CI Framework* adoption by NSF cyberinfrastructure operators.

Trusted CI has realized great success in the creation of cohorts surrounding adoption of the *Trusted CI Framework*. These cohorts have provided the camaraderie, motivation, and support that Major Facilities have needed to successfully adopt the *Framework*, and have provided Trusted CI with an effective means of efficiently and effectively supporting numerous Major Facilities simultaneously. These cohorts then continue their efforts through graduation into a Community of Practice. To address Must 10, Trusted CI will continue its work with the *Framework* Communities of Practice while also beginning one or two additional communities of practice, including at least one in software assurance.

Resources

Under the heading of *Resources*, Trusted CI seeks to address the topics of Adequate Resources, Budget, Personnel, and External Resources.

11. Adequate Resources: Organizations must devote adequate resources to address unacceptable cybersecurity risk.
12. Budget: Organizations must establish and maintain a cybersecurity budget.
13. Personnel: Organizations must allocate personnel resources to cybersecurity. Personnel resources are commitments made by an organization to assign human effort to cybersecurity.
14. External Resources: Organizations must identify external cybersecurity resources to support the cybersecurity program.

Trusted CI has historically performed surveys of cybersecurity budgets, addressing Musts 11 and 12. Trusted CI will continue this practice going forward. Trusted CI will also develop and implement a new budget training curriculum to provide for the community.

Trusted CI has significant existing activities in workforce development, addressing Musts 11 and 13 (personnel resourcing). These include its events, such as the NSF Cybersecurity Summit; along with Trusted CI Fellowships; partnerships, such as with other Centers of Excellence; and a student program associated with the Summit.

Trusted CI will continue and also particularly seek to expand its activities surrounding Musts 11 and 13 going forward as well. Notably, this will include a major push surrounding diversity in numerous areas: the Trusted CI team itself, participation in our activities, including Fellows, the Summit, and our student program. To facilitate success with this new push, Trusted CI will seek partnerships with minority-serving institutions (MSIs), in collaboration with the Minority Service Cyberinfrastructure Consortium (MS-CC). In conjunction with this, it will also seek to expand the student program, so that it is not centered solely around the Summit, and will entail activity throughout the year as well as internships and career opportunities involving placement at Major Facilities. Trusted CI will also grow its Fellows program. Additional diversity-focused initiatives will include training events at MSIs, security program development engagements with MSIs, and a possible MSI *Framework* Cohort.

Trusted CI will also continue to facilitate Must 14, including the creation of knowledge via guides such as the Software Guide, the Guide to Securing Operational Technology, and case studies. Going forward, as it has for the past few years, this creation of knowledge will be facilitated in large part through Trusted CI's Annual Challenges. Trusted CI's partnerships, including coordination with ResearchSOC and REN-ISAC are also vital for supporting external resources for NSF cyberinfrastructure operators.

Controls

Finally, Trusted CI will continue its activities surrounding controls, addressing Musts 15 and 16.

15. Baseline Control Set: Organizations must adopt and use a baseline control set.
16. Additional & Alternate Controls: Organizations must select and deploy additional and alternate controls as warranted.

This includes Trusted CI' existing efforts in IT assessments and engagements. Going forward, this will expand to include "residencies" that enable deeper embedding and support with Major Facilities that need this level of involvement from Trusted CI. It will also include an expanded effort in cybersecurity for regulated research. Going forward, and increase in software assurance will also be necessary, in response to the increasing amount of software — particularly in software automation and "self-driving labs" that are becoming common elements of NSF scientific discovery.

6 References

6.1 External

[JAS19] JASON. *Fundamental Research Security*, JSR-19-2I, December 2019. https://beta.nsf.gov/research-security

[JAS21] JASON. *Cybersecurity at NSF Major Facilities*, JSR-21-10E, October 2021. https://www.nsf.gov/news/special_reports/jasonreportcybersecurity/

[JAS23] JASON. *Research Program on Research Security*, JSR-22-08, March 2023. Available from: https://beta.nsf.gov/research-security

[MRZ+23] H. G Martin, *et. al*. Perspectives for Self-Driving Labs in Synthetic Biology. *Current Opinion in Biotechnology*, 79:102881, 2023. DOI: 10.1016/j.copbio.2022.102881

[NAS12] National Academies of Sciences, Engineering, and Medicine. *Earth Science and Applications from Space: A Midterm Assessment of NASA's Implementation of the Decadal Survey*, 2012. DOI: 10.17226/13405

[NAS13] National Academies of Sciences, Engineering, and Medicine. *Solar and Space Physics: A Science for a Technological Society*, 2013. DOI: 10.17226/13060

[NAS15] National Academies of Sciences, Engineering, and Medicine. *Sea Change: 2015-2025 Decadal Survey of Ocean Sciences*, 2015. DOI: 10.17226/21655

[NAS18] National Academies of Sciences, Engineering, and Medicine. *Visions into Voyages for Planetary Science in the Decade 2013-2022: A Midterm Review*, 2018. DOI: 10.17226/25186

[NAS19a] National Academies of Sciences, Engineering, and Medicine. *Management Models for Future Seismological and Geodetic Facilities and Capabilities: Proceedings of a Workshop*, 2019. DOI: 10.17226/25536

[NAS19b] National Academies of Sciences, Engineering, and Medicine. *An Astrobiology Strategy for the Search for Life in the Universe*, 2019. DOI: 10.10.17226/25252

[NAS19c] National Academies of Sciences, Engineering, and Medicine. *A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis*, 2019. DOI: 10.17226/25335

[NAS20] National Academies of Sciences, Engineering, and Medicine. *A Vision for NSF Earth Sciences 2020-2030: Earth in Time*, 2020. DOI: 10.17226/25761

[NAS21] National Academies of Sciences, Engineering, and Medicine. *Pathways to Discovery in Astronomy and Astrophysics for the 2020s*, 2021. DOI: 10.17226/26141

[NAS22a] National Academies of Sciences, Engineering, and Medicine. *Automated Research Workflows for Accelerate Discovery: Closing the Knowledge Discovery Loop,* 2022. DOI: 10.17226/26532

[NAS22b] National Academies of Sciences, Engineering, and Medicine. *Physics of Life,* 2022. DOI: 10.17226/26403

[NAS22c] National Academies of Sciences, Engineering, and Medicine. *Origins, Worlds, and Life: A Decadal Strategy for Planetary Science and Astrobiology*, 2022. DOI 10.17226/26522

[NAS23] National Academies of Sciences, Engineering, and Medicine. *Toward a 21st Century National Data Infrastructure: Enhancing Survey Programs by Using Multiple Data Sources*, 2023. DOI: 10.17226/26804

[NSB20] National Science Board. *Vision 2030*, NSB-2020-15, May 2020.

[NSF17] S. Anderson, E. Deelman, M. Parashar, D. Petravick, and E. M. Rathje. *NSF Large Facilities Cyberinfrastructure Workshop*, v6, November 2017

[NSF19] E. Deelman, I. Baldin, B. Bockelman, A. Bolton, P. Brady, T. Cheatham, L. Christopherson, R. Ferreira da Silva, T. Gulbransen, K. Keahey, M. Kogan, A. Mandal, A. Murillo, J. Nabrzyski, V. Pascucci, S. Petruzza, M. Rynge, S. Sons, D. Stanzione, C. Surajit, D. Swensen, A. Szalay, D. Thain, J. Towns, C. Vardeman, J. Wyngaard. *2019 NSF Workshop on Connecting Large Facilities and Cyberinfrastructure: Connecting Large Facilities, Connecting CI, Connecting People*, 2020, DOI: 10.25549/0ZBF-8M77

[NSF21a] A. Blatecky, D. Clarke, J. Cutcher-Gershenfeld, D. Dent, R. Hipp, A. Hunsinger, A. Kuslikis, and L. Michael. *The Missing Millions: Democratizing Computation and Data to Bridge Digital Divides and Increase Access to Science for Underrepresented Communities*, National Science Foundation report, October 2021. https://www.rti.org/publication/missing-millions/fulltext.pdf

[NSF21b] U.S. National Science Foundation. *Research Infrastructure Guide*, NSF 21-107, December 2021.

[NSF22] U.S. National Science Foundation. *Leading the World in Discovery and Innovation, STEM Talent Development and the Delivery of Benefits from Research - NSF Strategic Plan for Fiscal Years (FY) 2022 - 2026*, NSF 22-068, 2022.

[NSF23] U.S. National Science Foundation. *Research Security at the National Science Foundation*. [Checked online 2023-05-07].

[Par18] M. Parashar, *Realizing a Cyberinfrastructure Ecosystem that Transforms Science and A Win-Win Approach to Supporting the Shared Missions of Research and Education Communities*, 2018 Internet2 Global Summit, May 8, 2018.

6.2 Trusted CI Publications

[TCI16] *Open Science Cyber Risk Profile (OSCRP)*, 2016. DOI: 10.5281/zenodo.7268749

[TCI18a] *The Trusted CI Framework*, 2018. https://www.trustedci.org/framework

[TCI18b] *The Trusted CI Vision for an NSF Cybersecurity Ecosystem And Five-year Strategic Plan (2019-2023)*, Apr. 2018. https://hdl.handle.net/2022/22178

[TCI18c] *Trusted CI Broader Impacts Report*, June 2018. https://hdl.handle.net/2022/22148

[TCI19a] Trusted CI Experiences in Cybersecurity and Service to Open Science. In *Proceedings of the Practice and Experience in Advanced Research Computing (PEARC)*, 2019. https://doi.org/10.1145/3332186.3340601

[TCI19b] *An Examination and Survey of Random Bit Flips and Scientific Computing*, Dec. 2019. http://hdl.handle.net/2022/24910

[TCI20a] *An Examination and Survey of Data Confidentiality Issues and Solutions in Academic Research Computing*. Sept. 2020. https://escholarship.org/uc/item/7cz7m1ws

[TCI20b] *Scientific Data Security Concerns and Practices: A survey of the community by the Trustworthy Data Working Group*, Dec. 2020. DOI: 10.5281/zenodo.3906865

[TCI21a] *The Trusted CI Framework Implementation Guide for Research Cyberinfrastructure Operators*, Mar. 2021. DOI: 10.5281/zenodo.4562447

[TCI21b] *The State of the Scientific Software World: Findings of the 2021 Trusted CI Software Assurance Annual Challenge Interviews*. Sept. 2021. https://hdl.handle.net/2022/26799

[TCI21c] *Guide to Securing Scientific Software*. Dec. 2021. DOI: 10.5281/zenodo.5777646

[TCI22a] *Findings of the 2022 Trusted CI Study on the Security of Operational Technology in NSF Scientific Research*. Jul. 2022. DOI: 10.5281/zenodo.6828675

[TCI22b] *Roadmap for Securing Operational Technology in NSF Scientific Research*. Nov. 2022. DOI: 10.5281/zenodo.7327987