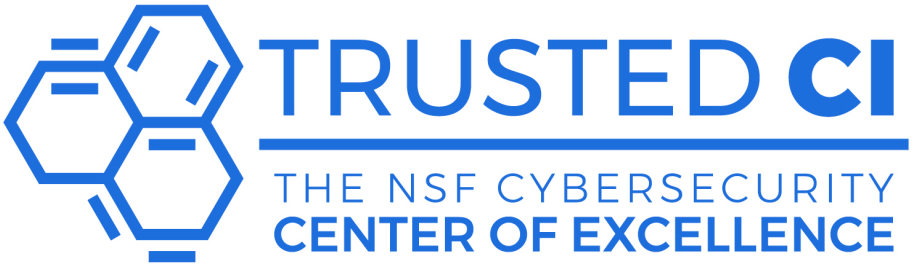

The Trusted CI Vision for an NSF Cybersecurity Ecosystem

And Five-year Strategic Plan

2019-2023

Version 1

June 20th, 2018

About this Document

This document is a product of Trusted CI, the NSF Cybersecurity Center of Excellence, trustedci.org.

This document is expected to evolve with subsequent revisions based on community feedback. Please send any comments to vwelch@iu.edu.

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, Trusted CI 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 was formerly known as the Center for Trustworthy Scientific Cyberinfrastructure (CTSC).

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

This report describes work supported by the National Science Foundation under Grant Number OCA-1547272. Any opinions, findings, conclusions, and 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/

Acknowledgments

We thank the Trusted CI Advisory Committee for their guidance on both this document and on Trusted CI's efforts generally: Tom Barton (U. Chicago & Internet2), David Halstead (NRAO), Neil Chue Hung (UK Software Sustainability Institute), Nicholas J. Multari (PNNL), Nancy Wilkins-Diehr (SDSC), and Melissa Woo (Stony Brook University). We also thank Sarah Engel (IU) for editing and numerous improvements of this document, and Craig Stewart (IU) and Ruth Aydt their review and suggestions.

The opinions expressed in this document do not necessarily reflect the opinions of any of the acknowledged parties.

Citing this Document

Please cite this document as follows:

> V. Welch, J. Basney, C. Jackson, J. Marsteller, and B. Miller, "The Trusted CI Vision for an NSF Cybersecurity Ecosystem And Five-year Strategic Plan (2019-2023)," Trusted CI, Apr. 2018 [Online]. Available: http://hdl.handle.net/2022/22178.

License

Table of Contents

1. Introduction

The National Science Foundation (NSF) funds over 11,000 awards each year with an annual budget of about $7.5 billion. These awards, in aggregate, create a science and engineering research community whose size and diversity is unparalleled. Implementing appropriate cybersecurity across this *NSF community* – in a way that is both effective in managing cybersecurity risks and enables this community to achieve its science objectives – is a complex interdisciplinary research challenge. Adding to this challenge is the reality that NSF awards are hosted in institutions (e.g., universities, research laboratories) that have their own diverse histories, policies, and risk tolerances with which the projects must comply.

Trusted CI, the NSF Cybersecurity Center of Excellence (CCoE)[1], has been working to overcome this challenge for over five years. Its success has been noted both by the NSF community, with the 2017 Report from the NSF Large Facilities Cyberinfrastructure Workshop [1] citing it as a model for future NSF centers and the 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." [2] (34:26)

This document establishes Trusted CI’s vision for a *NSF Cybersecurity Ecosystem* – a collection of people, knowledge, processes, and cyberinfrastructure – that is necessary to support cybersecurity across the diverse NSF community. Trusted CI is primarily responsible for bringing the vision of a NSF Cybersecurity Ecosystem to fruition. Hence, following Trusted CI’s vision is its mission statement and five-year strategic plan to fulfill that role.

[1] Trusted CI was formerly known as the Center for Trustworthy Scientific Cyberinfrastructure (CTSC).

2. Background

Trusted CI's vision for a NSF Cybersecurity Ecosystem exists to support NSF's Vision, the science missions missions of NSF projects, and NSF cyberinfrastructure (CI).

The NSF Vision, Big Ideas, and Diverse Research Community

NSF, in its strategic plan for 2018-2022 [3], establishes the NSF Vision of "a nation that is the global leader in research and innovation." The examples in the strategic plan, and the referenced 10 Big Ideas document [4], demonstrate the large diversity of research that NSF funds from its seven different science directorates. For example: harnessing the data revolution, exploring the new arctic, multi-messenger astrophysics, quantum computing, and phenotypes. This vision and breadth of research topics set challenging goals in terms of what NSF Cybersecurity Ecosystem must support.

Trustworthy Science

Cybersecurity is the practice of managing risks in order to achieve a goal. In this case, the goal is trustworthy science, that is research results that are reproducible and trusted by the scientific community and the public. Clearly trustworthy science requires more than cybersecurity to achieve – data curation, ethics, scientific method, etc. – but with research's heavy reliance on computing, specifically cyberinfrastructure (CI), cybersecurity is a necessary component.

Trusted CI has identified the following aspects of cybersecurity as important to trustworthy science:

1. **Availability**: Ensuring that cyberinfrastructure and scientific data results are available so that research can be productively accomplished and its results disseminated. For example, protecting instruments from cyber threats that make them unusable [5].
2. **Integrity**: Ensuring that data and data-producing infrastructure are not influenced by unauthorized parties. This includes being able to provide evidence to judge claims that research may have tampered with when data management practices are called into question (e.g., defending climate research [6]).
3. **Confidentiality:** Ensuring that research involving sensitive data protects that data from unauthorized disclosure. This includes data regulated by law as well as data sensitive due to ethical concerns (e.g., keeping the location of endangered species from poachers [7]).

NSF Cyberinfrastructure

Most scientific research relies heavily on computing, and NSF provides a large quantity of computing for science in the form of cyberinfrastructure (CI) [8]. NSF funds CI primarily through the same grant mechanisms it uses for science research, leading a large number and diversity of CI projects. Examples include software development done through the NSF Software Infrastructure for Sustained Innovation program and coordinated by software institutions [9], projects providing compute resources (e.g., the

Open Science Grid [10], Extreme Science and Engineering Discovery Environment [11], Jetstream [12], Wrangler [13]), and projects providing data storage and access (e.g., Big Data Regional Innovation Hubs [14]).

NSF also funds CI cybersecurity projects to provide expertise and technology to these projects to manage their cyber risks. This includes Trusted CI, which is funded as the NSF Cybersecurity Center of Excellence [15]. In a recent call for proposals [16], NSF has also indicated its intention to fund a Collaborative Security Response Center (CSRC), whose presumed existence is included in Trusted CI's Strategic Objectives later in this document.

In addition to NSF-funded CI, the NSF community benefits from shared IT and cybersecurity services where such make sense. Hence, NSF projects use software, infrastructure, and services from their hosting institutions (universities, research laboratories, etc.), regional networks (e.g., Quilt [17]), national organizations (e.g., Internet2 [18]), commercial services, and open source software.

3. The Trusted CI Vision: A NSF Cybersecurity Ecosystem

The NSF community is large and diverse, encompassing NSF itself, its seven science directorates, over two dozen Large Facilities, and tens of thousands of smaller ephemeral projects. This community is tightly integrated with the 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.

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. Even *Large Facilities*, the largest of the NSF projects, struggle to develop tailored approaches.

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

> "A NSF cybersecurity ecosystem, formed of people, practical knowledge, processes, and cyberinfrastructure, that enables the NSF community to both manage cybersecurity risks and produce trustworthy science in support of NSF's vision of a nation that is the global leader in research and innovation."

Trusted CI's vision of the NSF Cybersecurity Ecosystem requires certain attributes in the key areas of knowledge, people, cyberinfrastructure, and processes. Each attribute reflects this future vision, rather than the status quo. The following subsections describe these needed attributes.

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 (e.g., the newly solicited NSF Collaborative Security Response Center) to fully realize.

Knowledge: Leadership in Supporting Research and Innovation

1. The 11,000+ **new projects funded by NSF each year quickly and effectively establish appropriate cybersecurity programs**. The enabling knowledge for establishing and maintaining a NSF cybersecurity program is readily available, efficiently consumed, and effectively applied. This will be facilitated by contributions to the NSF Large Facilities Manual [19].

2. NSF Principal Investigators and Program Officers **know what resources are required to implement, maintain, and evaluate a cybersecurity program** appropriate for a project's science mission and size.

3. The relationship of NSF science to cybersecurity standards (e.g., NIST CSF, NIST RMF,, 800-171, HIPAA) is well understood and articulated. The community **shapes the application of cybersecurity standards to enhance the ability to do trustworthy science**.

4. **Cybersecurity lessons learned are shared across the NSF community** to build a corpus of knowledge and guard against knowledge loss as projects end. Social barriers have diminished, so the community heralds sharing lessons learned as well as successes.

5. The NSF community convenes discussions and **shares cybersecurity knowledge with other research communities and with the broader cybersecurity community.**

People: A Diverse, Well-Supported Workforce

1. NSF CI professionals, cybersecurity professionals, and researchers have **ready access to the cybersecurity professional development for NSF science** they need to be an effective workforce.

2. Workforce development efforts ensure the NSF Cybersecurity Ecosystem has **a talent pipeline, with people with diverse perspectives**, sufficient to effectively serve the entire NSF community.

3. The **information security offices at hosting institutions, regional networks, and national entities collaborate with NSF projects to best support their science missions**. The collaboration may be direct or through research computing facilitators. As cybersecurity becomes increasingly crucial, these interactions increase in both number and importance.

4. To gather requirements and broadly disseminate tailored cybersecurity guidance, the **NSF Cybersecurity Ecosystem collaborates with NSF centers of expertise and other key organizations**, e.g., the NSF software Institutes [9], XSEDE [11], OSG [10], the Coalition for Academic Scientific Computation [20], Internet2 [18], the Research and Education Networking Information Sharing and Analysis Center [21], and the NSF Large Facilities Office [22].

Cyberinfrastructure: Enabling People and Collaboration

1. **The NSF Cybersecurity Ecosystem takes advantage of advances to cybersecurity from research**. This includes research by NSF (e.g., Secure and Trustworthy Cyberspace [23]) as well as research by other organizations (e.g., Authentication and Authorisation framework for Research and Collaboration [24], WISE [25], Department of Homeland Security Science and Technology [26]). Through adoption of research, **the NSF Cybersecurity Ecosystem is a contributor to NSF's efforts to transition research to practice**.

2. **Guidance exists to leverage IT services from outside of the NSF community in a trustworthy manner.** The NSF community benefits from shared IT (e.g., cloud computing, storage, and high-level applications) where such sharing makes sense. This includes cybersecurity services from outside the community (e.g., InCommon [27], OmniSOC [28]).

3. **The NSF Cybersecurity Ecosystem deploys and operates its own tailored cybersecurity services when most effective**. Building on the experience of Trusted CI [29], XSEDE [30], and the new NSF Collaborative Security Response Center [16], new cybersecurity services will be established when appropriate.

4. **The NSF community readily discerns the operational and cybersecurity maturity of cyberinfrastructure components** in order to appropriately deploy them. Cyberinfrastructure is often born as a research product and later matures to support higher operational and cybersecurity standards. For example, software may start as research in itself, suitable for experimentation, but not hardened for deployment in mature operational contexts. As it proves itself useful to research, the software is matured, with application of professional engineering and security, enabling it for use in contexts of increasing risk.

5. **The NSF Cybersecurity Ecosystem enables interoperability and collaborative research with other agencies (Department of Energy, National Institutes of Health, etc.), nations, and entities** through coordination and collaboration.

Processes

1. **The NSF Cybersecurity Ecosystem works together closely in times of need** – for example, in response to incidents that broadly impact the community, or in response to administrative pressures on the community to adopt cybersecurity measures that must be adapted for scientific productivity.

2. **The NSF Cybersecurity Ecosystem recognizes a need for local autonomy and accommodation of diverse NSF projects in different areas of science, with different needs for collaboration, and at different points in their life cycle and hence maturity.**

3. **The NSF Cybersecurity Ecosystem recognizes the need for different risk tolerances.** Individual NSF projects have their own mission, maturity level, cultural risk tolerances, and existence within institutions with different cybersecurity programs.

4. **The NSF Cybersecurity Ecosystem collaboratively continues to define the five-year cybersecurity vision** to track changes in NSF science, the practice of cybersecurity, external threats, and cyberinfrastructure itself. Given the rapidly evolving nature of research, information technology and cybersecurity in particular, the ecosystem evolves with these changes.

4. The Trusted CI Mission and Strategic Objectives

Since 2012, NSF has funded Trusted CI, the NSF Cybersecurity Center of Excellence (trustedci.org)[2] to provide the scientific community with leadership and practical guidance in cybersecurity and related topics such as identity management and privacy. The center's accomplishments [31] include:

- 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.
- Educating the NSF community on cybersecurity's role in trustworthy and reproducible science.
- Impacting nearly 200 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.
- Producing freely available guidance on cybersecurity programs and identity management that has enabled at least ten NSF projects to develop their own programs in these areas.
- Launching a monthly webinar series on NSF cybersecurity which drew over 160 attendees and 80 subsequent viewings of recordings in its first year.
- Providing dozens of cybersecurity training sessions to hundreds of community members on topics such as identity management, log analysis, and secure coding.
- Re-establishing and growing the annual NSF Cybersecurity Summit to well over 100 attendees each year.

Trusted CI has primary responsibility for bringing the Trusted CI Vision for an NSF Cybersecurity Ecosystem to fruition. Hence, its new mission statement to support its vision:

> "The Mission of Trusted CI is to lead in the development of a NSF Cybersecurity Ecosystem with the workforce, knowledge, processes, and cyberinfrastructure that enables trustworthy science and NSF's vision of a nation that is a global leader in research and innovation."

To accomplish this mission, we organize the planned activities of Trusted CI under a set of strategic objectives, detailed in the subsequent sections. Trusted CI's overall metric of success will continue to be positive feedback from the NSF community. Each strategic objective is followed by a key metric of success we believe is essential to maintaining that community endorsement.

Strategic Objective 1: Build and Disseminate the Needed Knowledge

Strategic Objective 1.1: Develop and support the adoption of the NSF Cybersecurity Framework

Trusted CI and its member organizations have been building and disseminating practical knowledge for the past five years, including the Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects [32], reports from the NSF Cybersecurity Summits [33]–[35], the Open Science

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

Cyber Risk Profile [36], the Information Security Practice Principles [37], and training across a wide range of NSF cybersecurity topics [38].

Given the increased focus on cybersecurity globally, it is of increasing importance that the NSF community be able to articulate how this knowledge aggregates to form a comprehensive cybersecurity framework and how that framework relates to other broadly known programs such as the NIST Cybersecurity Framework [39] and NIST 800-171 [40]. **Trusted CI will accomplish this task by building on existing materials and developing new materials, integrated into a coherent framework appropriate to the NSF Cybersecurity Ecosystem**, thereby giving the NSF community the ability to resist less relevant frameworks.

Key metric of success: Adoption of the NSF Cybersecurity Framework by NSF Projects.

Strategic Objective 1.2: NSF Community Awareness

NSF funds over 11,000 projects a year. Assuming only those receiving over one million dollars in funding require some form of cybersecurity project, that means five hundred new projects every year need to quickly learn and apply the knowledge that Trusted CI is creating. **Trusted CI will be aggressive in evangelizing to these projects about the NSF Cybersecurity Framework, related cybersecurity resources, and workforce development opportunities Trusted CI and collaborating projects such as the CSRC provide.** This includes Trusted CI continuing to work with NSF, particularly the Large Facilities Office, to incorporate the NSF Cybersecurity Framework into NSF's guidance [19].

Key metric of success: Percentage of >$1M NSF projects each year consuming some product of Trusted CI.

Strategic Objective 1.3: Build the Community needed for the NSF Cybersecurity Ecosystem

Trusted CI will build and lead the community needed for the NSF Cybersecurity Ecosystem to be successful. **Trusted CI will continue to organize the annual NSF Cybersecurity Summits, online discussions, and communication forums** to continue to mature and grow the community. Community building will be done in collaboration with other NSF cybersecurity centers and projects. When other projects have a clear leadership mandate in an area, Trusted CI will support their efforts (e.g., it will assist the NSF Collaborative Security Response Center with coordinating incident response).

Key metric of success: Collaborations between NSF projects related to cybersecurity.

Strategic Objective 1.4: Continue to Deepen The Community's Understanding of Trustworthy Science

Before Trusted CI, much of the NSF community held the assumption that cybersecurity was a barrier to the mission of NSF science. **Trusted CI will continue to evangelize a flexible approach to cybersecurity, which balances baseline practices with risk management emphasizing the mission of scientific research**. This teaches the community that science and cybersecurity are not mutually exclusive, and

helps move project practices from avoiding cybersecurity to embracing it. Trusted CI must continue to develop the community understanding of how cybersecurity can be a supportive, enabling tool for productive, trustworthy research.

Key metric of success: Positive references to Trusted CI products by the NSF scientific community.

Strategic Objective 2: Processes to Sustain the Community

Strategic Objective 2.1: Effective Assistance and Sustainability

Trusted CI has provided over two dozen NSF projects with tailored consulting through its Engagement program [41]. Some of these Engagements have been funded under its grants from NSF and others directly by the projects (e.g., SGCI[3], ImPACT[4]). **Trusted CI will continue to improve its delivery of NSF- and project-funded Engagements** to most effectively and efficiently meet the needs of the NSF community. It will also continue to explore Engagements funded by projects as a means to the goal of achieving financial sustainability.

Key metric of success: Number of NSF projects paying Trusted CI directly for service.

Strategic Objective 2.2: Define Metrics and Track Progress

The NSF community needs metrics to track and ensure progress in implementing cybersecurity. **Trusted CI will lead the definition and tracking of cybersecurity community metrics** to achieve multiple goals: 1) Measure the impact of Trusted CI; 2) Enable community members to benchmark their efforts in relation to the cybersecurity efforts of other community members; 3) Demonstrate the maturation of the NSF Cybersecurity Ecosystem over time. When metrics are in the area of leadership of other NSF cybersecurity centers, Trusted CI will collaborate with those projects in defining and tracking the metrics.

Key metric of success: Improvement of metrics over time.

Strategic Objective 3: Secure Cyberinfrastructure

Strategic Objective 3.1: Improve the Security of NSF Cyberinfrastructure

In NSF community surveys conducted by Trusted CI [42], all responding projects indicated they undertake the development of at least some of the software they utilize. NSF funds the development of a large amount of software that becomes cyberinfrastructure. Currently there are no defined expectations on how to discern software that is itself research versus software that is sufficiently mature for use in operations, nor how software evolves along this spectrum. **Trusted CI will continue its work in developing secure software engineering and secure coding practices** [43]**.** These practices will provide

[3] NSF Award 1547611
[4] NSF Award 1659367

NSF-funded software development efforts and the broader NSF community with expectations on maturing software from a cybersecurity perspective and the knowledge to do so.

Key metric of success: Adoption of Trusted CI secure software practices by NSF projects.

Strategic Objective 3.2: Coordinate with the NSF CSRC

NSF, in solicitation 18-547 Cybersecurity Innovation for Cyberinfrastructure [16], has expressed its intent to fund a NSF Collaborative Security Response Center (CSRC). This center will bolster the NSF Cybersecurity Ecosystem by building community incident response capabilities. **Trusted CI will coordinate and collaborate with the new CSRC to foster the success of both centers and the ecosystem.** For example, Trusted CI will work with the NSF CSRC to explore collaboration on the annual NSF Cybersecurity Summit, defining and tracking metrics, and exploring which operationally-focused activities of Trusted CI will be shifted to the NSF CSRC (e.g., Trusted CI's current Cyberinfrastructure Vulnerabilities [44] awareness service).

Key metric of success: Number and continuity of synergistic activities with the NSF CSRC.

Strategic Objective 3.3: Service Coordination and Delivery

NSF projects can benefit from incorporating outside cybersecurity services within their cybersecurity programs (e.g., from the higher education community or the private sector). Some of these services are relatively generic (e.g., software testing), while others may need to be tailored to the NSF community (e.g., the Collaborative Security Response Center laid out in the 2018 CICI solicitation [16]). **Trusted CI will tailor, as needed, and vet third party services to best address the needs of the NSF community** – ultimately serving as the trusted source for identifying which services are well positioned to serve NSF project needs and working to improve services for the NSF community. In the case of services focused on operational security, the CCoE will coordinate with the NSF CSRC.

Key metric of success: Number of cybersecurity services utilized by NSF projects.

Strategic Objective 3.4: Build a National Community around Cybersecurity for Research

The NSF community collaborates both nationally (e.g., Department of Energy, National Institutes of Health) and internationally (e.g., Large Hadron Collider, Square Kilometer Array, Laser Interferometer Gravitational-Wave Observatory). **Trusted CI will play a leadership role in coordinating with outside organizations to ensure effective collaboration** by building trust with the NSF community and aligning technical services (perhaps in collaboration with the NSF CSRC).

Key metric of success: Successful coordination of events with non-NSF organizations.

Strategic Objective 4: Foster the Workforce and Collaborations

Strategic Objective 4.1: Workforce Development and Training

Trusted CI will continue to provide high-quality training for the NSF community. Trusted CI's training will be broadly and readily available through in-person and online means. Training will be tailored for the various stakeholders in the community (e.g., cybersecurity professionals, project management, researchers, and leadership).

Metric of success: Training attendance and feedback.

Strategic Objective 4.2: Workforce Inclusion and Recruitment

Trusted CI and other NSF projects need cybersecurity professionals to accomplish the work described in these strategic objectives. That workforce needs to be constantly refreshed to adjust for growth, departures, and changes in projects. **Trusted CI will continue efforts to make students and non-NSF professionals aware of the NSF Cybersecurity Ecosystem and the opportunities to work in cybersecurity and enable science**, an exciting combination. **Increasing the representation of minorities and underrepresented groups in the NSF Cybersecurity Ecosystem**, whose demographics at NSF Cybersecurity Summits indicate a white male majority, will serve to bolster the workforce.

Metrics of success: Outreach events. Increased minority representation in the NSF Cybersecurity Ecosystem.

Strategic Objective 4.3: Outreach to Higher Education

With over 11,000 funded projects per year and, by interpolation, tens of thousands of funded projects at any time, Trusted CI is significantly challenged to impact all these projects and address their cybersecurity needs. Trusted CI needs to seek leverage, and two promising sources are research facilitators (e.g., Coalition for Academic Scientific Computation, the CaRC Consortium, Advanced Cyberinfrastructure Research and Education Facilitators) and information security offices. **Trusted CI will continue outreach to higher education information security offices and research facilitators to enable them to help NSF projects with cybersecurity.** Today both lack key expertise – cybersecurity in the case of of the research facilitators, and an understanding of NSF project engagement in the case of the information security offices. Trusted CI's outreach will cover these areas of expertise and encourage collaboration between these two groups.

Key metric of success: Positive feedback from information security offices, research facilitators, or NSF projects on successful engagements between these groups.

Strategic Objective 4.4: Build a Network of Cybersecurity Fellows

To further address the challenge of impacting the tens of thousands of NSF funded projects, Trusted CI will establish a Trustworthy CI Fellowship program. This program will establish and support a network of Fellows with diversity in both geography and scientific discipline. These fellows will have access to

training and other resources to foster their professional development in cybersecurity. In exchange, they will champion cybersecurity for science in their scientific and geographic communities, and communicate challenges and successful practices to Trusted CI.

Key metric of success: Coverage of scientific disciplines and geographic areas by Trusted CI Fellows.

Strategic Objective 4.5: Cybersecurity Transition to Practice

The NSF Secure and Trustworthy Cyberspace (SaTC) [23] and Cybersecurity Innovation for Cyberinfrastructure (CICI) [45] programs regularly produces cutting edge cybersecurity research and development results. **Trusted CI will continue to act as a communication conduit between the SaTC, CICI and NSF communities** (e.g., via cybersecurity workshops [46]). In this role, Trusted CI will foster the transition of this research and development into practice in the NSF community and convey unmet cybersecurity requirements back to the research and development communities as targets for future research.

Key metric of success: Examples of transition of research to practice or challenges to research.

5. Conclusion

This document has put forth Trusted CI's vision for a NSF Cybersecurity Ecosystem – a collection of people, knowledge, processes, and cyberinfrastructure – that is necessary to support cybersecurity across the diverse NSF community. This vision is based on Trusted CI's five years of working on the challenge of cybersecurity for NSF science. A new mission statement is proposed for Trusted CI as the entity primarily responsible for realizing the vision. The mission statement is refined with a set of strategic objectives, providing details and metrics of success for how Trusted CI will fulfill the mission. The strategic objectives structure Trusted CI's planned activities, and include key metrics of success – metrics that will ultimately help the NSF research community transition cybersecurity research to practice, implement a comprehensive cybersecurity program based on a newly developed NSF Cybersecurity Framework, and draw on best practices from the broader R&E community.

6. References

[1] S. Anderson, E. Deelman, M. Parashar, D. Petravick, and E. M. Rathje, "NSF Large Facilities Cyberinfrastructure Workshop," v6, Nov. 2017 [Online]. Available: http://facilitiesci.org/

[2] 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," 08-May-2018 [Online]. Available: https://meetings.internet2.edu/2018-global-summit/detail/10004995/. [Accessed: 11-Jun-2018]

[3] "National Science Foundation: Investing in Science, Engineering, and Education for the Nation's Future. Strategic Plan for 2014 – 2018," Mar. 2014 [Online]. Available: https://www.nsf.gov/pubs/2014/nsf14043/nsf14043.pdf

[4] "NSF's 10 Big Ideas - Special Report | NSF - National Science Foundation." [Online]. Available: https://www.nsf.gov/news/special_reports/big_ideas/. [Accessed: 05-Mar-2018]

[5] N. Perpitch, "How cyber attackers almost stole a unique chance from Australian astrophysicists," *ABC News*, Australian Broadcasting Corporation, 17-Oct-2017 [Online]. Available: http://www.abc.net.au/news/2017-10-17/cyber-attack-almost-costs-team-look-at-colliding-neutron-stars/9055816. [Accessed: 01-Apr-2018]

[6] M. B. Seth Borenstein, "Major global warming study again questioned, again defended," 07-Feb-2017 [Online]. Available: https://phys.org/news/2017-02-major-global-defended.html. [Accessed: 01-Apr-2018]

[7] R. Kondos, "From binoculars to big data: Citizen scientists use emerging technology in the wild," *O'Reilly Media*, 05-Jul-2017. [Online]. Available: https://www.oreilly.com/ideas/from-binoculars-to-big-data-citizen-scientists-use-emerging-technology-in-the-wild. [Accessed: 01-Apr-2018]

[8] "About Advanced Cyberinfrastructure | NSF National Science Foundation." [Online]. Available: https://www.nsf.gov/cise/oac/about.jsp. [Accessed: 01-Apr-2018]

[9] "NSF commits $35 million to improve scientific software | NSF - National Science Foundation." [Online]. Available: https://www.nsf.gov/news/news_summ.jsp?cntn_id=189347. [Accessed: 06-Mar-2018]

[10] "Open Science Grid." [Online]. Available: https://www.opensciencegrid.org/. [Accessed: 06-Mar-2018]

[11] "Home - XSEDE." [Online]. Available: https://www.xsede.org/. [Accessed: 06-Mar-2018]

[12] "Jetstream: A National Science and Engineering Cloud." [Online]. Available: https://jetstream-cloud.org/. [Accessed: 01-Apr-2018]

[13] "Wrangler - Texas Advanced Computing Center." [Online]. Available: https://www.tacc.utexas.edu/systems/wrangler. [Accessed: 01-Apr-2018]

[14] "Big Data Regional Innovation Hubs and Spokes Workshop | NSF - National Science Foundation." [Online]. Available: https://www.nsf.gov/cise/bdspokes/index.jsp. [Accessed: 01-Apr-2018]

[15] "Trusted CI: the NSF Cybersecurity Center of Excellence," *Trusted CI: the NSF Cybersecurity Center of Excellence*. [Online]. Available: https://trustedci.org/. [Accessed: 01-Apr-2018]

[16] "nsf18547 Cybersecurity Innovation for Cyberinfrastructure (CICI)," *National Science Foundation*, 07-Mar-2018. [Online]. Available: https://www.nsf.gov/publications/pub_summ.jsp?ods_key=nsf18547. [Accessed: 16-Mar-2018]

[17] "Home - The Quilt," *The Quilt*. [Online]. Available: https://www.thequilt.net/. [Accessed: 01-Apr-2018]

[18] "Home | Internet2." [Online]. Available: https://www.internet2.edu/. [Accessed: 01-Apr-2018]

[19] Prepared by the Large Facilities Office in the Budget, Finance, and Award Management Office (BFA-LFO), "NSF Large Facilities Manual," Mar. 2017 [Online]. Available: https://www.nsf.gov/pubs/2017/nsf17066/nsf17066.pdf
[20] "Coalition for Academic Scientific Computation." [Online]. Available: http://casc.org/. [Accessed: 06-Mar-2018]
[21] "REN-ISAC," *REN-ISAC*. [Online]. Available: https://www.ren-isac.net/. [Accessed: 01-Apr-2018]
[22] "Office of Budget, Finance, and Award Management: Large Facilities Office (LFO) | NSF - National Science Foundation." [Online]. Available: https://www.nsf.gov/bfa/lfo/. [Accessed: 06-Mar-2018]
[23] "Secure and Trustworthy Cyberspace (SaTC)." [Online]. Available: http://www.nsf.gov/pubs/2016/nsf16580/nsf16580.htm. [Accessed: 01-Sep-2016]
[24] "AARC." [Online]. Available: https://aarc-project.eu/. [Accessed: 01-Apr-2018]
[25] "WISE Community – Wise Information Security for Collaborating E-infrastructures." [Online]. Available: https://wise-community.org/. [Accessed: 01-Apr-2018]
[26] "Science and Technology," *Department of Homeland Security*, 12-Nov-2014. [Online]. Available: https://www.dhs.gov/science-and-technology. [Accessed: 01-Apr-2018]
[27] "InCommon: Security, Privacy and Trust for the Research and Education Community." [Online]. Available: https://www.incommon.org/. [Accessed: 01-Apr-2018]
[28] "OmniSOC." [Online]. Available: https://omnisoc.iu.edu/. [Accessed: 01-Apr-2018]
[29] "Cyberinfrastructure Vulnerabilities," *Trusted CI: the NSF Cybersecurity Center of Excellence*. [Online]. Available: https://trustedci.org/vulnerabilities/. [Accessed: 01-Apr-2018]
[30] "Security - XSEDE." [Online]. Available: https://www.xsede.org/ecosystem/operations/security. [Accessed: 01-Apr-2018]
[31] J. Dopheide, J. Zage, and J. Basney, "The Trusted CI Broader Impacts Project Report (pending)," Trusted CI, 2018 [Online]. Available: http://hdl.handle.net/2022/22148. [Accessed: 21-Jun-2018]
[32] Jim Marsteller, Craig Jackson, Susan Sons, Jared Allar, Terry Fleury, Patrick Duda, "Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects, v1," Center for Trustworthy Scientific Cyberinfrastructure, Aug. 2014 [Online]. Available: https://scholarworks.iu.edu/dspace/handle/2022/20026. [Accessed: 18-Jun-2017]
[33] J. Marsteller, V. Welch, and A. Starzynski Coddens, "The Report of the 2016 Cybersecurity Summit for Large Facilities and Cyberinfrastructure: Strengthening Trustworthy Science," Dec. 2016 [Online]. Available: https://scholarworks.iu.edu/dspace/handle/2022/21161. [Accessed: 19-Mar-2018]
[34] C. Jackson, J. Marsteller, A. Starzynski Coddens, and V. Welch, "Report of the 2015 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure," Nov. 2015 [Online]. Available: https://scholarworks.iu.edu/dspace/handle/2022/20539. [Accessed: 19-Jun-2017]
[35] C. Jackson, J. Marsteller, and V. Welch, "Report of the 2014 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure," Dec. 2014 [Online]. Available: https://scholarworks.iu.edu/dspace/handle/2022/19244. [Accessed: 19-Mar-2018]
[36] S. Peisert *et al.*, "Open Science Cyber Risk Profile (OSCRP)," 2017 [Online]. Available: https://scholarworks.iu.edu/dspace/handle/2022/21259. [Accessed: 19-Mar-2018]
[37] Craig Jackson, Scott Russell, and Susan Sons, "The Information Security Practice Principles," Version 0.9, May 2017 [Online]. Available: https://cacr.iu.edu/principles/ISPP-Foundational-Whitepaper-2017.pdf
[38] "Trusted CI Training Materials," *Trusted CI: the NSF Cybersecurity Center of Excellence*. [Online]. Available: https://trustedci.org/trainingmaterials/. [Accessed: 19-Mar-2018]
[39] "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, Feb. 2014 [Online]. Available: https://www.nist.gov/cyberframework. [Accessed: 01-Apr-2018]
[40] A. R. R. (nist), A. K. D. (nist), A. P. V. (nara), A. M. R. (nara), and A. G. G. (ida), "SP 800-171 Rev. 1,

Protecting CUI in Nonfederal Systems and Organizations | CSRC." [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final. [Accessed: 01-Apr-2018]

[41] "Engaged Communities," *Trusted CI: the NSF Cybersecurity Center of Excellence*. [Online]. Available: https://trustedci.org/engagedcommunities/. [Accessed: 19-Mar-2018]

[42] R. Cowles and C. Jackson, "2016 NSF Community Cybersecurity Benchmarking Survey Report," 2016 [Online]. Available: https://scholarworks.iu.edu/dspace/handle/2022/21355. [Accessed: 06-Sep-2017]

[43] J. A. Kupsch, B. P. Miller, E. Heymann, and E. César, "First Principles Vulnerability Assessment," in *Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop*, Chicago, Illinois, USA, 2010, pp. 87–92 [Online]. Available: http://doi.acm.org/10.1145/1866835.1866852

[44] "Vulnerabilities," *Trusted CI: the NSF Cybersecurity Center of Excellence*. [Online]. Available: https://trustedci.org/vulnerabilities/. [Accessed: 21-Mar-2018]

[45] "Cybersecurity Innovation for Cyberinfrastructure | NSF - National Science Foundation." [Online]. Available: https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=505159. [Accessed: 21-Jun-2018]

[46] "IU hosts cybersecurity workshop to help opposites attract," *IU hosts cybersecurity workshop to help opposites attract*. [Online]. Available: https://itnews.iu.edu/articles/2017/iu-hosts-cybersecurity-workshop-to-help-opposites-attract.php. [Accessed: 01-Apr-2018]