

PROJECT SUMMARY

Overview:

Trusted CI, as the NSF Cybersecurity Center of Excellence, provides the NSF community with strategic leadership and immediate assistance in tackling cybersecurity challenges and implementing cybersecurity in support of trustworthy, reproducible science. It provides the community with cybersecurity best practices and a cybersecurity framework tailored for science, and supported by training, webinars, and presentations to empower the community to implement robust yet appropriate cybersecurity programs to support their scientific missions. It engages directly with NSF projects to tackle their cybersecurity challenges and hosts the annual NSF Cybersecurity Summit, which is open to the community.

Intellectual Merit:

Trusted CI is leading the NSF science community in tackling a set of cybersecurity challenges stemming from its open and collaborative research, using distributed and high-performance cyberinfrastructure across heterogeneous science domains and project sizes, and with an emphasis on data integrity. These attributes result in cybersecurity needs that require careful selection, tailoring, or the creation of cybersecurity frameworks and controls. The community needs training and guidance to implement a cybersecurity program around those controls. The value of cybersecurity to science productivity and reproducibility must be compelling to motivate adoption. Trusted CI's cybersecurity transition to practice program is tackling the communication and other barriers to connect researchers with practitioners to benefit both.

Broader Impacts:

Trusted CI builds on a history of helping nearly 200 projects from across all seven NSF science directorates. It gathers requirements, collaborates on its analyses, and disseminates its products through a strong network of collaborators that includes the regional networks across the U.S., a Fellows program, and partnerships with other flagship NSF centers and projects. Woven into all of Trusted CI's activities is the inclusion of populations and regions that are underrepresented in cybersecurity.

CICI: CCoE: Trusted CI: Advancing Trustworthy Science

A. Proposal Overview: Trusted CI as Community Partner and Leader

Over the past six years, Trusted CI pioneered and set the standard for an NSF Cybersecurity Center of Excellence (CCoE) through continuous innovation in cybersecurity and cultivating the NSF community's trust in Trusted CI as a partner and a leader. **Trusted CI has thus far helped nearly 200 projects improve their cybersecurity posture.** Trusted CI's funding for this role is primarily provided by NSF award 1547272. We propose Trusted CI be funded under this CICI solicitation [1] to continue as the CCoE in order to continue our leadership and build on our significant contributions to the field. Trusted CI's continued leadership as the NSF CCoE will maintain the community's momentum and collaborative tackling of its cybersecurity challenges, and prevent increasing the risk of society losing trust in over seven billion dollars of NSF-supported science during a particularly tumultuous time.

Based on our successful history, our forward-looking five-year vision for the NSF CCoE [2] captured in this proposal will sustain and improve upon our existing efforts to advance trustworthy, reproducible NSF science. Highlights of our vision include: 1) leading the community in the expansion and adoption of a comprehensive cybersecurity framework to support the NSF and open science, adopted across the U.S. and internationally; 2) creating a cybersecurity fellows program that expands our impact across the seven NSF science directorates [3], the NSF Big Ideas [4], and underrepresented segments of the community; 3) initiating an innovative training program in cybersecurity for science in collaboration with the Quilt [5] and regional networks across the U.S.; and 4) tackling, in collaboration with other community leaders, an annual challenge to trustworthy science, starting with data integrity.

Trusted CI will successfully accomplish these activities and achieve powerful impacts through **strong collaborations and community engagement as described in our 40 supplemental letters of collaboration.** These collaborations demonstrate our community ties and include NSF Large Facilities [6] (NSF's most significant commitments to scientific infrastructure), the NSF Big Data Innovation Hubs [7], cybersecurity researchers, the Science Gateways Community Institute [8], the NSF CI Center of Excellence Pilot [9], NSF Engagement and Performance Operations Center [10], the Quilt [5], 11 regional networks, and international entities.

B. The Need for Trusted CI as the NSF CCoE

Scientific infrastructure and cyberinfrastructure (CI) continues to be the victim of cyberattacks and scientific data theft (e.g., [11–16]), and is under scrutiny in terms of its security by Congress (e.g., [17, 18]). **These cybersecurity concerns both hinder productivity and bring into question the trustworthiness and reproducibility of supported science.** The solicitation [1] calls out the challenges for cybersecurity presented by NSF-funded cyberinfrastructure: providing an open, collaborative, highly distributed environment, with highly heterogeneous infrastructure. This environment must efficiently produce science that is trusted by the scientific community and the public in the face of cybersecurity threats, both targeted at science and indiscriminately at IT infrastructure. As indicated by community contributions to the NSF's CI2030 report [19], each science project has particular cybersecurity and risk management needs emerging from its size, local university policies, collaborations, infrastructure, data, and other variables. Research computing centers also wrestle with compliance (e.g., [20]). The community needs both a vision to tackle cybersecurity as well as appropriate training and guidance to implement it in a manner than balances and promotes scientific productivity. Perhaps most importantly, cybersecurity needs to be presented to project leadership as something that fosters trustworthy science, rather than as something that creates a barrier to it.

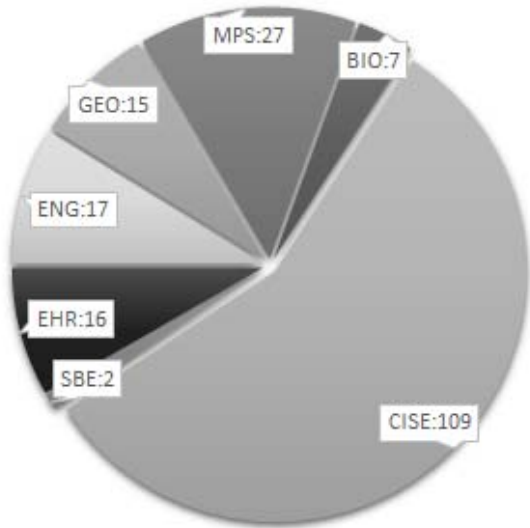
Hence, **cybersecurity for NSF cyberinfrastructure is a complex challenge in understanding requirements, community engagement, community building, policies, procedures, incentives, and selective, careful adaptation and application of cybersecurity practices from the broader community.** Individual NSF projects do not have the resources to tackle this challenge in a sustained, interoperable manner. An NSF CCoE is needed to: 1) continue to advance the understanding of how cybersecurity benefits trustworthy and reproducible science, 2) tackle challenges arising from emerging technology paradigms (e.g., the increasing use of cloud computing [21], which leaves cybersecurity a responsibility of projects using it), 3) distill actionable guidance that balances risk and scientific productivity, and 4) provide leadership and help the community organize itself.

C. Results of Prior Support

The Trusted CI PI and co-PIs have been successfully working together in their current roles leading an NSF CCoE – formerly known as the Center for Trustworthy Scientific Cyberinfrastructure (CTSC) – for the past six years under awards 1234408 (10/1/2012-9/30/2016, \$4,518,845) and 1547272 (1/1/2016-6/30/2020, \$7,829,993). During this time, we **successfully prototyped and proved the value of an NSF CCoE with a demonstrated ability to establish the community’s trust, create a shared understanding of the role of cybersecurity in science, and empower the community through best practices and training to implement effective cybersecurity.** Publications: [22–31].

Intellectual Merit: Our accomplishments include providing the community with a guide and templates for developing and maintaining a cybersecurity program [27], authoring and submitting to NSF a draft section on information security for the draft NSF Major Facilities Guide [32], and developing and providing training on a variety of cybersecurity topics [33]. Success is indicated by the 2017 NSF Large Facilities Cyberinfrastructure Workshop report citing Trusted CI as being “viewed as a great example of a community resource” [34], the NSF Large Facilities Office [6] listing Trusted CI as a resource, positive feedback from engaged projects as shown in the callout box on the next page, and being lauded by the director of the NSF Office of Advanced Cyberinfrastructure as “a very innovative model in providing cybersecurity expertise to NSF large projects such as the NSF Facilities and has been extremely successful.” [35 (34:26)]

Broader Impact: As detailed in our Broader Impacts Report [36] and our annual reports to the NSF [37–43], we restarted the NSF Cybersecurity Summits [22, 23, 25, 28–30], nearly doubling initial attendance from 69 in 2013 to 117 in 2018; started a webinar series [44] with a total viewership (live and recorded) of 1,500; engaged with 44 NSF projects to address their cybersecurity challenges; delivered over 120 hours of training in 2017 [36]; established the NSF Large Facilities Security Team [45] with members from 22 NSF Large Facilities meeting monthly; and delivered best practices, in collaboration with the community, in identity and access management [46], risk management [24], cybersecurity program development [27], and cloud service hosting [31]. In total, as described by the Broader Impacts Report [36] and shown in Figure 1, **Trusted CI impacted nearly 200 NSF projects across all seven NSF science directorates** [3]. Additionally, our efforts resulted in articles regarding cybersecurity for science reaching a broad audience (e.g., [47–53]), an NSF webinar on cybersecurity for science [54], and a cybersecurity presence at PEARC [55], the NSF SI2 PI meeting [56], and Science Gateways conference [57]. Trusted CI organized, in collaboration with STEM-Trek [58], the URISC workshop at SC17 [49, 59] with 34 participants from 11 sub-Saharan African countries and representatives from underserved regions of the U.S. across 12 states. Trusted CI supported the formation of the Minority Serving Cyberinfrastructure Consortium (MS-CC) [60] and seeks out opportunities to empower underrepresented groups (e.g., [61–64]).

<p>Community feedback from Trusted CI Engagements (from its annual reports [37–43])</p> <p><i>"Our security posture, policy framework and overall cybersecurity program have improved considerably as a result of the engagement."</i> - Gemini Observatory (\$21m annual budget [65])</p> <p><i>"The most immediate outcome of our engagement with CTSC [Trusted CI] has been an improvement in our security posture."</i> - IceCube (\$7m annual budget [65])</p> <p><i>"With their support we were able to meet the deadline with a revised modern Cybersecurity plan."</i> - LSST (\$50m annual budget [65])</p>	 <p>Figure 1: Trusted CI has impacted 193 projects across all seven NSF directorates [36].</p> <table border="1"> <thead> <tr> <th>Directorate</th> <th>Number of Projects</th> </tr> </thead> <tbody> <tr> <td>CISE</td> <td>109</td> </tr> <tr> <td>MPS</td> <td>27</td> </tr> <tr> <td>ENG</td> <td>17</td> </tr> <tr> <td>GEO</td> <td>15</td> </tr> <tr> <td>EHR</td> <td>16</td> </tr> <tr> <td>SBE</td> <td>2</td> </tr> <tr> <td>BIO</td> <td>7</td> </tr> </tbody> </table>	Directorate	Number of Projects	CISE	109	MPS	27	ENG	17	GEO	15	EHR	16	SBE	2	BIO	7
Directorate	Number of Projects																
CISE	109																
MPS	27																
ENG	17																
GEO	15																
EHR	16																
SBE	2																
BIO	7																

D. Our Proposed Work: Continued Community Service and Leadership

In the following sections, we describe Trusted CI’s proposed activities. Each section starts with the specific solicitation criteria it addresses. Given that our current activities are effective and relied upon by our community, and given that the budget available under this solicitation of \$2.5 million per year is comparable to Trusted CI’s current budget, much of our proposed work represents improvements to current activities. However, Trusted CI balances this stability with continued innovation to increase our impact. **Innovations new to this proposal are the international collaboration around a cybersecurity framework for science in Section D.1, the Annual Challenges also in Section D.1, and the collaboration with the Quilt and Regionals in Section D.9.** Relatively new, having just been launched by Trusted CI in 2019 under a supplemental award, are the Fellows Program (Section D.2), the work extending the Open Science Cyber Risk Profile (Section D.7), and the cybersecurity research transition to practice program (Section D.10).

The final section, D.13, provides overall metrics for Trusted CI’s success in fostering productive, trustworthy, reproducible science, as well as our Community Benchmarking Survey we use to measure our overall impact. This section complements metrics at the conclusion of each section specific to the activities in that section. Our Project Plan, provided as a supplement document as requested by the solicitation, provides additional details on timing and management.

D.1. Providing Leadership for Cybersecurity for Science

Solicitation criteria: “Provide leadership to the NSF research community in the continuous building and distribution of a body of knowledge on the topic of trustworthy cyberinfrastructure” and “address the challenges in balancing security constraints and risk management with the scientific process, including access to data for scientific researchers.”

Providing leadership is the cornerstone of Trusted CI’s mission [2]: “The Mission of Trusted CI is to lead in the development of an 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.” Two Trusted CI activities are focused on leadership as well as balancing security and productive science: the Trusted CI Framework and the Annual Challenges.

The Trusted CI Framework: An Architecture for Cybersecurity Programs will be a cybersecurity framework appropriate for scientific cyberinfrastructure that balances risk reduction with scientific productivity, and has the necessary flexibility for the NSF’s diverse community. Or, in other words, to achieve for the NSF community the Federal Cybersecurity R&D Strategic Plan’s goal [66] to “make cybersecurity less onerous while providing more-effective defenses.” Key to the Framework’s success will be its acceptance as an alternative or complement to other cybersecurity frameworks or control sets (e.g., NIST 800-171 [67]). Scientific projects and research computing centers are often pressured to adopt such control sets, which can be detrimental to scientific productivity without adding suitable risk management for the mission of science [54, 68].

Achieving such success will be a multi-year effort of development, socialization, early adoption, and working with the community to solicit and incorporate feedback. We have started the Framework from our successful “Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects” [27], a product that influenced the NSF’s draft Major Facilities Guide (MFG) [32] (formerly the Large Facilities Manual [69]) chapter on cybersecurity. To foster adoption, we will engage heavily with NSF higher education communities and collaborating organizations across the globe. Specifically, we will work with NSF Large Facilities (the Large Facilities Security Team described in Section D.4), research computing leaders (see letter from the Campus Research Computing Consortium [70]), and higher education information security leaders (leveraging our connections through the ResearchSOC, described in Section D.6) to share drafts and incorporate feedback, and then to foster adoption. There is a strong need for such a framework in the science community as indicated by letters of collaboration from the Wise Information Security for E-infrastructure Community [71], Gemini [72], IceCube [73], LSST [74], the National Solar Observatory [75], NEON [76], NERSC [77], ESnet [78], Australia’s National Computational Infrastructure [79], and the Australian National University Cyber Institute [80]. We will continue to provide suggestions regarding cybersecurity to the NSF Large Facilities Office [6] to continue their evolution of the Major Facilities Guide and keep these documents in alignment.

We expect the Framework effort will span the full five years of this proposed work. During each of those years, we will also take on an **Annual Challenge**, a cybersecurity challenge to reproducible, trustworthy science that is unlikely to be addressed without our leadership. Our first challenge is the issue of data integrity. As called out in the Federal Cybersecurity R&D Strategic Plan [66], “In many situations, integrity and availability are the dominant properties of interest,” and data integrity is a particular challenge for trustworthy, reproducible science as large data sizes are surpassing protections in our current IT infrastructure [51, 81–85]. Data integrity is also not well addressed in many cybersecurity control sets (e.g., NIST 800-171 is focused on confidentiality). Some science projects already undertake their own data integrity protections, but there is no community consensus on the risks to scientific results, or guidance to projects for protecting integrity. This makes a consensus for data integrity critical, particularly as data infrastructure is growing (“Harnessing the Data Revolution” is one of the NSF’s 10 Big Ideas [4]).

Following the model that successfully produced prior guidance (e.g., [24, 31]), Trusted CI will collaborate with the four NSF Big Data Innovation Hubs [7], the NSF CI CoE Pilot [9], the Ostrom Workshop on Data Management and Information Governance [86], the NSF Engagement and Performance Operations Center [10], the Indiana Geological and Water Survey [87] (see supplied letters of collaboration). This collaboration will survey key science projects to determine the spectrum of integrity concerns and practices already in place. That data will be analyzed and broadly applicable guidance will be produced for science projects and CI developers. We will use our events and social media channels (see Sections D.4 and D.11) to disseminate this guidance. That outreach, in combination with number of contributing

projects, should give the guidance sufficient visibility and gravitas to be noticed by the NSF community and have impact.

Following data integrity, Trusted CI will focus on a different challenge each year that has similar attributes of being critical to trustworthy, reproducible NSF science, and is at risk of not being addressed by the broader world outside of the NSF. Our tentative topics, which will be adjusted or even replaced as necessary based on changes in the NSF environment and conversations with our advisory committee and the NSF, are:

- **Software assurance:** As described in Section D.12, the NSF community both produces and consumes software from a variety of sources. Today, little understanding exists of how to evaluate and manage risks in these software supply processes. A year-long effort collaborating with key stakeholders, including the CI CoE Pilot [9] (see letter from Dr. Deelman), to form and appropriately disseminate software producers and consumers, educators, and the NSF is needed to develop consensus and guidance for the NSF community and drive adoption.
- **Sensor and control systems security:** Numerous NSF projects use sensors and control systems to gather data or control instruments. This usage is highly diverse (e.g., ecological [76], urban [88], astronomy [72], natural disasters [89]) and, similar to integrity, risks and practices need to be gathered and analyzed to produce broadly applicable guidance to the community.
- **Scalable cybersecurity auditing:** NSF funds over 11,000 projects each year [90]. Trusted CI engages with many projects, but needs new community engagement paradigms to impact at this scale. We will enable and foster “peer reviews” – cybersecurity audits carried out between projects without outside mediation – by providing ground rules and processes for projects to audit each other’s cybersecurity programs. Trusted CI has already facilitated such audits [91] and with a focused effort will formalize this guidance such that reviews can be undertaken without requiring Trusted CI’s assistance, allowing for great scalability.
- **Identity and Access Management:** Trusted CI continues to see strong demand from NSF projects and facilities for assistance with identity and access management (IAM). For example, Trusted CI engagements with the Environmental Data Initiative (EDI - DBI-1565103 & DEB-1629233) and the Scalable Amplified Group Environment (SAGE2 - ACI-1441963) projects in 2018 both focused on IAM aspects. As the NSF CI2030 report notes: “Efforts to simplify identity management must continue...” [19]. IAM is a core component of the Trusted CI Framework and is a common area of focus for our Science Gateways Community Institute (SGCI) collaboration (e.g., our January 2019 SGCI IAM webinar [92]). A year-long focus on this topic will include presentations/tutorials (Internet2 Technology Exchange, PEARC, Gateways, Cybersecurity Summit) and updated materials (implementation guides, policy templates, webinars, etc.) in collaboration with InCommon/Internet2 and SGCI.

For the first year’s Annual Challenge, we have our aforementioned partners lined up. For years two through five, we will finalize the topics in discussions with our advisory committee and the community, and then build an appropriate collaboration (our collaborators for year one provide strong evidence that we have suitable connections throughout the community to regularly achieve this community building).

Key metrics of success: Adoption of the Trusted CI Framework and guidance resulting from Annual Challenges by NSF projects measured annually through our Community Benchmarking Survey.

D.2. Applying Best Cybersecurity Practices to Enable Trustworthy Science

Solicitation criteria: “Apply that knowledge and leverage relationships to increase the understanding of and adoption of best practices for trustworthy science” and “Ensure adoption of security best practices in the NSF research community.”

As described in the previous section, Trusted CI will collaboratively develop and carefully select cybersecurity best practices. Their adoption is not only a matter of making sure the practices are reasonable and effective, but also that NSF projects are aware of them and the leadership of those projects sees their value. Our ongoing outreach processes (Section D.4) and the annual Cybersecurity Summit (Section D.11) will be key to achieving adoption. We will further bolster our community engagement and adoption with the **Trusted CI Open Science Cybersecurity Fellows Program**. This program is being modeled after the successful UK Software Sustainability Institute (SSI) Fellowship Programme [93]. UK SSI director Neil Chue Hong, already on the Trusted CI Advisory Committee [94], is advising this effort. Dr. Dana Brunson is part of Trusted CI Leadership Team and has significant experience in this form of community building from leading the Campus Champion program [95] – a community of practice of campus research computing professionals comprising 530 individuals from 272 institutions covering every state and EPSCoR jurisdiction [96].

Each year, six Fellows will be recruited, trained, and mentored, joining a growing cohort of Fellows and giving Trusted CI growing impact and visibility across the NSF community. The Fellows will be recruited from the scientific community via an advertised open call distributed extensively to wide audiences, including, but not limited to: NSF directorates under-impacted by Trusted CI, Campus Champions [95], CaRC [70], CASC [97], Society of Women Engineers (SWE) [98], Society of Hispanic Professional Engineers (SHPE) [99], XSEDE (especially the Broadening Engagement program [100]), HPCWire [101], Science Node [102], the Strategic Partnership for Advanced Cyberinfrastructure at MSIs [60], and the Trusted CI project members’ respective communications offices. Criteria for Fellows will intentionally be very inclusive. Envisioned Fellows include an IT professional working on an NSF project, a campus research computing facilitator, or a campus information security professional.

Fellows will receive recognition, cybersecurity professional development consisting of training and mentorship from members of the Trusted CI team, and travel funding. The Fellows’ training will consist of a Virtual Institute, providing 20 hours of basic cybersecurity training over six months. The training will be delivered by Trusted CI staff and invited speakers, presenting selected introductory training material developed by Trusted CI [33] plus other introductory material developed by PI Welch’s team (e.g., the CyberCamp [103]). The Virtual Institute will be presented as a weekly series via Zoom [104] and recorded to be publicly available for later online viewing. Each Fellow will be provided a mentor from the Trusted CI team to provide extra support and guidance. Travel support is budgeted to cover Fellows’ attendance at the NSF Cybersecurity Summit (with an in-person meeting of the Fellows) [105], PEARC [55], and one professional development opportunity agreed to with Trusted CI. The Fellows will have a monthly call and be added to an email list to discuss any challenges they encounter that will receive prioritized attention from Trusted CI staff. Trusted CI will recognize the Fellows on its website and social media.

After the Virtual Institute, Fellows, with assistance from the Trusted CI team, will be expected to help their scientific community with cybersecurity and make them aware of Trusted CI for complex needs. By the end of each year, they will be expected to present or write a short white paper on the cybersecurity needs of their community and share some initial steps they will take (or have taken) to address these needs. After the year of full support, Trusted CI will continue recognizing the cohort of Fellows and giving them prioritized attention.

Key metrics of success: Number and diversity (NSF directorate, project size, gender and ethnicity, etc.) of applicants. Reported benefit of Fellowship from applicants via annual follow-up survey.

D.3. Engagements: Critical Tailored Aid to the NSF Community

Solicitation criteria: “Conduct security audits and security architecture design reviews for projects at multiple scales, from large Major Research Equipment and Facilities Construction (MREFC) projects to small CI developments”

Conducting security audits and design reviews will continue to be a core Trusted CI activity through its “Engagements” [106]. Engagements are typically six-month collaborative activities between the project and a small team of Trusted CI staff. The goal is to assess some aspect of the project’s cybersecurity or otherwise tackle a cybersecurity-related challenge of the project, and provide the project with actionable, prioritized guidance. When the engaged project is comfortable with publication, final reports from these engagements are published (e.g., [18, 19]). Otherwise, they are kept private between Trusted CI and the project.

Over the past six years, **Trusted CI has engaged with forty-four NSF projects of all sizes to address their cybersecurity challenges**, including helping DKIST [107], OOI [108], LSST [109], IceCube [73], LTER [110], UNHRCC [111], and TransPAC [112] to develop their cybersecurity programs; conducting cybersecurity program reviews for Array of Things [88], Design Safe [89], Gemini Observatory [72], HUBzero [113], NRAO [114], and USAP [115] and performing risk assessments for CyberGIS [116] and NEON [76]. Other engagements addressed student training through the NSF Scholarship for Service program [117], documentation of best practices (with Agave [118], CyVerse [119], and Jetstream [120]), software assessments (GenApp [121]), OSG/HTCondor-CE [122], and Globus [123]), and identity and access management (DataONE [124]), LIGO [125], OSIRIS [126], SciGaP [127], Wildbook [128], and perfSONAR [129]). A full list of Trusted CI’s engagements may be found in Section 6 of its most recent annual report to the NSF [37].

Demand from the community for Engagements has exceeded Trusted CI’s capability to deliver them, so Trusted CI provides a twice-per-year open engagement application process [130]. Since establishing the application process in 2016, five calls for applications have resulted in 36 applications being received, with 18 being accepted (we combined some applications into a single engagement when their needs overlapped). The Trusted CI Leadership Team (see Section E) judges the applications based on criteria of Need (will the engagement result in more trustworthy, reproducible science), Broader Impact (will the results be helpful to other projects and, to be added, does the requesting project represent underrepresented populations – e.g., is the project in an EPSCOR state [96] or Minority Serving Institution [131]), and Applicant Commitment (does the project demonstrate sufficient management support and resources to follow through with the engagement results). Trusted CI Leaders with a conflict of interest in an application do not participate in judging it.

Trusted CI will continue to provide these engagements via our application process to at least six projects per year. We will continue to evaluate our application process and consider incorporating outside expertise and reviewers as demand increases. And, as described in Section D.1, we will use an Annual Challenge to foster peer reviews to allow the community to scale these engagements on their own.

Additionally, Trusted CI partners with the CI Center of Excellence (CoE) Pilot [9] (NSF award #1842042, PI Deelman) and the Science Gateways Community Institute [8] (SGCI, NSF award #1547611, PI Wilkins-Diehr), to co-fund, with each, a shared .5 FTE focusing on cybersecurity for their respective communities. Activities under these collaborations are mutually agreed to with the partners and allow Trusted CI to have community engagement and impact with these centers’ communities.

Key metrics of success: Number of engagements provided to the community. Number of engagements requested. Number of projects providing direct financial support to Trusted CI.

D.4. Ongoing Outreach: Webinars, Office Hours, Social Media, Training

Solicitation criteria: “Offer weekly ‘office hours’ to the community to provide short-term consulting services” and “Address how the awardee will use collaboration tools or social media to disseminate cybersecurity information and best practices to the NSF community.”

In order to ensure the NSF community is aware of Trusted CI's services and to advance the community's understanding of the importance of cybersecurity to science, Trusted CI maintains a number of social media outreach channels – a website [132], webinar series [44], a blog [133], email lists [134], a Twitter feed [135], and a YouTube channel [136] – frequently presents [137] and provides training [33], with preference given to events that seek to increase inclusion by underrepresented groups (e.g., [59, 61–64]), and seeks out media appearances [47–53]. The average live attendance for the webinar in 2018 was 24 attendees per webinar, and views of recorded presentations on YouTube from 2017 and 2018 were approximately 70 views per webinar, with **a total of over 1500 views of the webinars from 2017 and 2018**. The Twitter account received approximately 82,000 Twitter impressions in 2018. The blog received approximately 18,500 page views in 2018. The website received approximately 7,700 visits in 2018.

In 2016, Trusted CI formed the Large Facility Security Team (LFST) [45], composed of individuals with cybersecurity responsibilities representing 22 (85%) NSF Large Facilities. Trusted CI will continue to lead the LFST, organizing monthly meetings featuring topics of interest (e.g., presentations on the European Union's General Data Protection Regulation [138] and Spectre/Meltdown [139] vulnerabilities were arranged at the request of the LFST). The LFST also provides valuable early feedback on Trusted CI recommendations, such as the Framework described in Section D.1. As the NSF increases its investments in Mid-scale Facilities and Infrastructures [4, 140], Trusted CI will monitor the needs of these projects and consider inviting them to join the LFST or set up a parallel group.

Trusted CI will continue all of these outreach mechanisms, and add weekly “office hours” via online chat (e.g., Slack [141]). Some office hours will have topics related to Trusted CI activities (e.g., follow-up from a webinar, discussion of a new Trusted CI report, or coordination following a situational awareness alert). Some office hours will not have a pre-set topic, but will be an open forum for community members to interact in real-time with available Trusted CI staff. Understanding that many cybersecurity topics cannot be addressed in just one hour, we expect the office hours to generate follow-up activities, such as blog posts, engagements, and webinars.

Key metrics of success: Number of participants in webinars and office hours. Number of blog writers and viewers.

D.5. Situational Awareness for Improved Risk Management

Solicitation criteria: “Provide situational awareness of the current cyber threats to the research and education environment, including those that impact scientific instruments.”

As called out by the Federal Cybersecurity R&D Strategic Plan [66]: “Timely, risk-relevant threat intelligence information sharing can improve organizations' abilities to assess and manage risks.” To provide the community with such intelligence, Trusted CI will continue to operate its freely available Cyberinfrastructure Vulnerabilities service [142], which provides concise announcements on critical vulnerabilities that affect CI, including those threats that may impact scientific instruments. **Trusted CI Cyberinfrastructure Vulnerabilities service has 108 subscribers, including 13 NSF Large Facilities.**

Community feedback from survey of Cyberinfrastructure Vulnerabilities subscribers:

"Having CTSC [Trusted CI] assess and advise on timely vulnerabilities allows my project another perspective from the CI community to compare against our own internal assessment, giving us greater confidence in our mitigation strategy."

"They help to highlight the important vulnerabilities among the flood of notices that we all receive every day."

"CTSC's [Trusted CI's] software vulnerability alerts often provide a secondary level of confidence for addressing concerns in a timely, if not priority, manner. They are an important community marker that should continue - thank you."

The Cyberinfrastructure Vulnerabilities service is operated in coordination with XSEDE [143], OSG [122], and the NSF supercomputing centers [144] to minimize duplication of effort and maximize the benefit from community expertise. We monitor a number of sources for vulnerabilities of interest, filter those of interest to the NSF community, and provide guidance on mitigating threats. The Traffic Light Protocol [145] is followed for responsible information sharing between collaborating projects.

Key metrics of success: Increase the number of subscribers to the mailing list. Engage new community projects to collaborate on providing this service.

D.6. Coordination with the ResearchSOC for Efficient and Effective Cybersecurity

Solicitation criteria: "Coordinate with the NSF-funded Collaborative Security Response Center (CSRC, which provides operational services and intelligence to NSF projects)"

Trusted CI PI Welch is also the PI on the NSF-funded CSRC, the Research Security Operations Center (ResearchSOC) [146] (NSF award #1840034). Co-PI Marsteller is similarly on both projects. As described in Appendix A of the latest Trusted CI annual report [37], Welch and Marsteller are committed to the projects appropriately leveraging each other's activities while respecting their complementary missions: ResearchSOC's to deliver operational cybersecurity services to NSF projects, and Trusted CI's to be a trusted advisor to motivate and empower NSF projects to adopt cybersecurity programs.

The projects will collaborate to ensure the Trusted CI Framework's (Section D.1) applicability based on ResearchSOC's operational cybersecurity experience. ResearchSOC will contribute content as well as draw requirements from the Cybersecurity Summit (Section D.10). ResearchSOC will leverage and adopt Trusted CI's best practices and training when appropriate. Both projects will contribute to the Cyberinfrastructure Vulnerability service (Section D.5), and will coordinate in reaching out to the higher education community, with Trusted CI taking the lead on reaching out to research computing centers (see Section D.9), and the ResearchSOC reaching out to information security groups and researchers.

Key metric of success: Number of collaborative efforts between the CCoE and ResearchSOC.

D.7. Refining the Science Threat Model and Countermeasures

Solicitation criteria: "...refine existing threat models identifying the vulnerabilities in NSF-funded cyberinfrastructure and scientific data associated with that cyberinfrastructure, and recommend countermeasures to protect the systems."

The Open Science Cyber Risk Profile (OSCRP) [24, 147–150] is a living and published document, developed by Trusted CI in collaboration with LBNL, ESnet [151], and a convened working group of research and education community leaders [152]. The OSCRP has been cited by several NSF solicitations and projects (e.g., [1, 153, 154]), and in the draft NSF Major Facility Guide [32]. The OSCRP is designed to help science project leadership and information technology professionals collaboratively

assess cybersecurity risks related to projects. It provides a mapping from common science assets to technology-based cybersecurity risks, facilitating conversations between scientists and information security professionals who are unfamiliar with each other's language.

While the OSCRP provides a methodology and initial set of science assets, it certainly is not comprehensive. We'll continue work started in 2019 to expand the OSCRP, tackling outputs from our Annual Challenges (Section D.1), findings from the NSF Cybersecurity Summits (Section D.11), cybersecurity incidents in the community, and community contributions. Countermeasures are challenging as they tend to be technology specific, and hence timely and of narrow applicability. We will add (and accept from the community via GitHub [150]) examples of countermeasures of greatest applicability.

Key metrics of success: Citations and uses of the OSCRP. Community Contributions to the OSCRP.

D.8. Interoperability in a Global Science Community

Solicitation criteria: "Coordinate with appropriate outside organizations in building trust with the NSF community and aligning technical services."

Trusted CI maintains numerous collaborations outside of the NSF community to ensure interoperability of its guidance and NSF CI. Collaborations include advisory committee members from higher education (Thomas Barton, Dr. Melissa Woo), the Department of Energy (Dr. Nick Multari), and the UK Software Sustainability Institute (Dr. Neil Chue Hong). Co-PIs Miller and Welch are also co-PIs in the DHS Software Assurance Marketplace [155]. Senior Personnel Jackson at Indiana University works with the Department of Defense (DoD) to apply Trusted CI-developed cybersecurity and engagement techniques within the DoD [156]. Additionally, as described in Section D.1, in order to assure broad adoption of our framework for science cybersecurity, we are collaborating with an impressive list of U.S. and international partners to receive contributions and feedback. This list includes the Department of Energy's Energy Sciences Network [78], the Wise Information Security for E-infrastructure Community [71], NERSC [77], Australia's National Computational Infrastructure [79], and the Australia National University Cyber Institute [80]. We also encourage select outsiders to attend the NSF Cybersecurity Summit, which has been attended by representatives from the Department of Energy, the National Institutes of Health, the Department of Homeland Security, Amazon, Google, and Microsoft. Our cybersecurity research transition to practice workshops (Section D.10) allow us to further engage the private sector (e.g., we have accepted Microsoft's offer to host our planned 2019 workshop).

Key metric of success: Number of institutions outside of the NSF community collaborated with each year.

D.9. Leveraging the Higher Education Community to Support Trustworthy Science

Solicitation criteria: "Engage with higher education structures through outreach to information security offices and research facilitators."

New to this proposal is a **powerful collaboration with the Quilt [5] to empower regional networks across the country in training their higher education membership in cybersecurity for research.** The Quilt membership consists of regional networks from across the U.S., whose membership in turn consists of higher education institutions of all sizes. As described in our letter of collaboration from Quilt President and CEO Jen Leasure, our collaboration takes the form of a "train the trainers" program at the Quilt annual meeting. We will provide materials and training to the regionals to train their higher education membership on how to provide cybersecurity for science on their respective campuses. The NSF Engagement and Performance Operations Center [10], per the letter from Dr. Jennifer Schopf, will contribute to this training.

We have commitments from 11 regional networks to attend the inaugural training (see supplemental letters from 3ROX, FRGP, GPN, iLight, KINBER, LONI, NEREN, NJEDge, NYSERNET,

OSHEAN, WVNET), evidence of the strong demand for this training and the opportunity for the regionals to get more from their membership. After the first year and tuning of the training based on feedback from the inaugural cohort, we will open the training up to all Quilt members and incrementally expand and improve the training. Given the breadth of the Quilt and the regionals, this will give Trusted CI broad impact across the U.S. (including numerous EPSCoR [96] states).

As we write this proposal, Dr. Dana Brunson, a member of our leadership team, is transitioning to a new role as Executive Director of Research Engagement at Internet2 [157]. Internet2 has a membership that includes 317 institutions of higher education [158]. Trusted CI will leverage this strengthened relationship, especially in areas of shared interest: identity and access management, and last-mile networking security (e.g., Science DMZs [159]). Internet2 will be invited to participate in Trusted CI engagements related to these shared interests. Trusted CI and Internet2 will meet at Internet2 Global Summits [160] to share opportunities, experiences, and successes, and to collaborate on dissemination to campuses.

Other relationships with the higher education community include:

- We work with **research computing centers** embedded in higher education institutions by providing training in compliance at the NSF Cybersecurity Summits (Section D.11), and they are a key stakeholder of the Trusted CI Framework described in Section D.1. We will leverage our relationships with the Campus Research Computing Consortium (see letter of collaboration from Dr. Tom Cheatham) and Internet2 (e.g., [161]) to engage with this community.
- Recognizing that many NSF projects are served by **information security professionals** in the project's hosting higher education institution, we undertake (along with the ResearchSOC as described in Section D.6) outreach to those professionals to educate them on how to engage with research projects, how to tackle the cybersecurity challenges those research projects are likely to have, and how to contact Trusted CI for more challenging cases (e.g., [92–94]).
- Per our letter of support from Prof. Cheshire, Prof. Webber, and Dr. Ashwin at University of California Berkeley, we will share our experiences regarding institutional mechanisms, organizational relationships, and interpersonal trust relationships with their NSF SaTC proposal team to foster their **research in cybersecurity coordination**.
- Prof. Miller and Dr. Elisa Heymann each receive funding from the University of Wisconsin-Madison to teach software security based on Trusted CI materials (Section D.13).
- **Workforce development through student engagement:** The NSF Cybersecurity Summit student program (Section D.11) brings six students to the summit each year. A student hourly position at Indiana University engages one student in Trusted CI activities. An ongoing collaboration with Cal Poly Pomona (see letter of support from Dr. Husain) enables nationwide outreach to students in the NSF Scholarship for Service (SFS) program [162]. E.g., we participated in Dr. Husain's 2017 annual workshop attended by 45 students from 13 different universities [117].

Key metrics of success: Number of regional networks trained. Number of higher education institutions trained by regionals and measured by follow-up survey. Count of NSF projects assisted by their institutional information security office as measured by our Community Benchmarking Survey (see D.13).

D.10. Accelerating Cybersecurity Research Transition to Practice (TTP)

Solicitation criteria: "Play a role in transition to practice of successful cybersecurity research results to eventual adoption and use of cutting-edge capabilities in scientific research."

Federal R&D spending in the cybersecurity arena remains a high national priority. Ensuring the transition of research into practice (TTP) of that research is essential to maximizing return on investments and protecting our scientific assets and national cyberinfrastructure. Accelerating TTP was a theme in the

2011 and 2016 Federal Cybersecurity Research and Development Strategic Plans [66, 163]. Our interactions with cybersecurity researchers indicate that many do not have access to practitioners to provide valuable feedback on their research, nor an understanding of how to communicate the value of their research to those practitioners. We hear of similar communication challenges from the practitioners.

Trusted CI is using its broad perspective and connections across the NSF CI community, cybersecurity practitioners, and cybersecurity researchers to foster TTP (e.g., [50, 164]). A concerted effort started in 2019 under funding from a supplement and with the addition of Florence Hudson to the leadership team. We identify cybersecurity needs and gaps through interviews and discussions (e.g., we organized a tabletop discussion at the 2018 NSF Cybersecurity Summit) with practitioners, including Chief Information Security Officers, cyberinfrastructure operators, industry, entrepreneurs, and the Large Facilities Security Team (Section D.4). Going forward, we expect to incorporate input from our Annual Challenges (Section D.1), Cybersecurity Fellows (Section D.2), and the ResearchSOC (Section D.6). To identify researchers who seem ready to transition to practice and whose research may address the identified needs and gaps, we review SaTC [165] awards and awards in NSF programs involved in TTP and research commercialization, such as Partnerships for Innovation (PFI) [166], iCORPS [167], and SBIR/STTR [168].

We then connect those researchers and practitioners through workshops we convene [50, 169, 170]. Preparation for the workshops includes coaching the researchers and providing valuable business modeling guidance to help them communicate a clear and concise value proposition to potential users to encourage operational piloting or adoption of the research. We leverage these workshops to have impact on underrepresented minority organizations in STEM and security as described in our Broader Impacts (Section G). For example, our planned 2019 event in Chicago will be in collaboration with Bunker Labs [171], a not-for-profit organization supporting U.S. veterans and military spouse entrepreneurs, and we have reached out to the Society of Women Engineers [172], Society of Hispanic Professional Engineers [173], National Society of Black Engineers [174], the Women In Technology Cyber Security & Technology Special Interest Group [175], and Women in Security and Privacy [196] to invite their members to join.

The University of South Alabama (under award NSF #1636470) also works to assist NSF researchers with TTP [176] and we have an agreement to collaborate by sharing experiences and attending each other's workshops (see letter from Dr. Yasinsac). We also communicate with the TTP program at the Department of Homeland Security (DHS) [177] to explore collaborative opportunities.

Key metrics of success: Number of NSF-funded cybersecurity research assets deployed into practice. Number of researchers and practitioners engaged (with count of underrepresented groups).

D.11. Community Building through the Annual Cybersecurity Summits

Solicitation criteria: "Host an annual conference in addition to meetings, seminars, training, and other events in order to interact with members of the NSF community, industry, government, and academia who wish to collaborate on projects and other initiatives."

In 2013, Trusted CI relaunched the NSF Cybersecurity Summits [22, 23, 25, 28–30] after a five-year hiatus, and have continued to organize successful annual summits for the NSF community. In 2014, Trusted CI introduced a Call for Participation that has been highly successful in setting the agenda and creating greater community involvement with the event. The summit also has brought in international collaborators to strengthen the NSF communities' global ties [178, 179]. **Summit attendance has nearly doubled from 69 in 2013 to 117 in 2018.**

We will continue to organize the annual Cybersecurity Summits, providing the opportunity for the NSF community to highlight cybersecurity challenges, build professional networks, receive training from Trusted CI and others, and have workshops and discussions to tackle common challenges. To foster

broader community attendance, we will move the summits geographically from their traditional location near Washington, D.C. Following the successful model of the Zeek project [180] (formerly “Bro”), each year we will solicit a summit host (if a suitable host does not emerge, Trusted CI members will host).

The summit will continue to support a successful student program that has received positive feedback from both students and mentors [181]. The program committee solicits and reviews all submissions with an interest in advancing diversity and inclusiveness. The six selected students are paired with mentors from the program committee and community to encourage their continued participation in cybersecurity and NSF cyberinfrastructure.

Key metrics of success: Summit attendance and feedback evaluations. Number of submitted presentations. Diversity of attendance by NSF directorate, gender, and ethnicity.

D.12. A Solid Foundation for Cyberinfrastructure: Software Assurance

Solicitation criteria: “A description of how CCoE will address software assurance should be included”

Software is being developed in significant quantity by the CI community (e.g., [182]). Producing software without weaknesses and vulnerabilities is a challenge due to technical barriers and a lack of incentives. Hence, this software can introduce significant risks to the operation of cyberinfrastructure and the science it supports. Trusted CI will continue working with both software developers and operators to help them measure and manage these risks by providing training and source code reviews. Trusted CI will continue **developing and delivering training in secure coding, secure software engineering, and software vulnerability assessment** at the NSF Cybersecurity Summit (Section D.11), Supercomputing [183], PEARC [55], and directly to institutions. The curriculum is tailored to the interests and technical needs of the audience. We will also continue to develop and offer new online training resources dedicated to software assurance [184]. These resources will expand on our secure programming curriculum to include secure software design, software assurance tools, system defenses, and in-depth software vulnerability assessment. **These same materials form the basis for an advanced undergraduate or introductory graduate class** on the Introduction to Software Security taught by Prof. Miller and Dr. Elisa Heymann, under separate funding from the University of Wisconsin-Madison. These materials are oriented to an active learning (flipped classroom) approach to instruction.

TrustedCI will continue to conduct Engagements (Section D.3) that involve an **in-depth review of a project’s source code**. These in-depth engagements apply our First Principles Vulnerability Assessment methodology [185] to understand and document the software’s structure, identify the high-value assets in the software, find specific vulnerabilities in the code, demonstrate these vulnerabilities with exploits, and then produce a comprehensive engagement report for use by the software development team.

Finally, as mentioned in Section D.1, we will devote one of our Annual Challenges to software assurance. The goal of a challenge is to engage the various stakeholders in the software supply chain to identify the key challenges for software assurance in the CI community, increase awareness of these issues, and produce a consensus as to how to most effectively address them. Trusted CI’s experience will be a key asset in this process, and the results will help inform Trusted CI’s directions.

Key metrics of success: Video modules, text chapters, and exercises produced. Number of venues and attendees trained. Number of students taking classes based on our materials. Number of downloads of relevant guidelines and best practices documents produced.

D.13. Measuring our Impact on Science

Solicitation criteria: "Proposals should provide appropriate metrics of success"

Each of the activity sections concludes with the metrics for that activity we will measure. In aggregate, these activities will combine to further Trusted CI's overall goal [2]: "...to lead in the development of an NSF Cybersecurity Ecosystem with the workforce, knowledge, processes, and cyberinfrastructure that enables trustworthy science and the NSF's vision of a nation that is a global leader in research and innovation." **Metrics for this overall goal are the levels of adoption of cybersecurity programs by the community, and maturity and confidence in those cybersecurity programs as demonstrated by our Community Benchmarking Survey [25, 26].** We will undertake the survey every other year (2021 and 2023), soliciting details from the community on the state of their cybersecurity program through our outreach channels (Section D.4). The results will then both serve to track our progress towards our goal and steer our activities.

Additionally, each year we will include updated impact metrics from the Broader Impacts report [36] in our annual report to the NSF [186]. The metrics analyze our impact in terms of the number of NSF projects we interact with and the distribution of those projects by NSF directorate. A secondary goal is to achieve impact across NSF directorates in proportion to their funding, and these reports will track this progress.

E. A Proven Team and Management Process

PI Welch has ultimate responsibility for Trusted CI's success. He is assisted by the Trusted CI Leadership Team composed of the co-PIs (Dr. James Basney, James Marsteller, and Prof. Barton Miller) and other senior team members (Dr. Dana Brunson, Florence Hudson, Mark Krenz, and Dr. Sean Peisert). The Trusted CI team has worked together effectively for six years and has strong, proven management processes that will continue. The Trusted CI team is highly respected and trusted by the NSF community. For example, Basney is PI of CILogon [187] and SciTokens [188], key identity management projects; Marsteller is co-lead for the XSEDE [143] Incident Response team and the XSEDE security office; Welch's team at Indiana University is funded to provide cybersecurity leadership for the Open Science Grid/IRIS-HEP (The Institute for Research and Innovation in Software for High Energy Physics) [122], a number of small NSF projects [189–191], the DHS Software Assurance Marketplace [155], and the PACT project in the Department of Defense [156]. Recently, PI Welch and co-PI Marsteller founded the ResearchSOC (Research Security Operations Center) [146], a second large operational NSF cybersecurity center. **The success of Welch and Marsteller in starting this second NSF cybersecurity center and the other examples provided in this paragraph are strong evidence of the respect and trust the NSF and broader communities places in Trusted CI's leadership.** As we describe in Section D.6, Trusted CI coordinates with the ResearchSOC to maximize value to the NSF community.

Trusted CI management is based on the processes described in Traction [192] (adopted from the Science Gateway Community Institute through our collaboration) and uses a six-month cycle of goal setting, engagement applications (Section D.3), and other activities determined necessary by the Leadership Team. Project plans are created for each activity, and progress is tracked via a red/yellow/green status reporting spreadsheet. Weekly Leadership Team meetings monitor the progress of engagements and projects and address any issues. Quarterly Leadership Team meetings set, monitor, and steer overall direction. Trusted CI holds a monthly all-hands meeting to debrief on completed activities and share lessons learned across the team. Since Trusted CI is a distributed team, most meetings are via videoconference (Zoom [104], provided institutionally by Indiana University). An annual all-hands in-person meeting is used to discern ways the project can improve, explore new means of serving the community, and set strategic goals for the year. Additionally, each activity and site involved in the project

holds its own meetings as needed. Google Docs [193] and GitHub [194] are used to share and collaborate. Trusted CI's cybersecurity program [195], updated annually, maintains the confidentiality, integrity, and availability of these and other project assets. As requested by the solicitation, specific milestones are described in our Project Plan.

PI Welch and the Leadership Team will continue to be guided by the Trusted CI Advisory Committee [94]:

- Tom Barton, Senior Consultant for Cyber Security and Data Privacy at the University of Chicago
- Eric Cross, Information Technology Manager at the National Solar Observatory
- Neil Chue Hong, Director of the UK Software Sustainability Institute (SSI)
- Nicholas J. Multari, Senior Project Manager for Research in Cyber Security at the Pacific Northwest National Lab (PNNL)
- Nancy Wilkins-Diehr, Associate Director at the San Diego Supercomputing Center, and PI of the NSF Science Gateways Community Institute (SGCI)
- Melissa Woo, Senior Vice President for Information Technology (IT) and Chief Information Officer at Stony Brook University.

The committee is consulted frequently (e.g., they reviewed early versions of our five-year vision [2], they receive copies of all quarterly and annual reports to the NSF, and they convene in person annually). At their annual meeting we accept their feedback on the previous year, present and discuss plans for the upcoming year, and have frank discussions regarding issues the Trusted CI leadership team is experiencing. Relevant NSF program officers are invited to attend, and feedback from the committee is shared with the NSF in addition to being considered in Trusted CI planning.

F. Intellectual Merit

Cybersecurity for scientific research has fundamental differences with cybersecurity for other “missions” and the institutions and people who perform those missions. The intellectual merit of this proposal is continuing to understand the evolving nature of scientific research, particularly its increasingly data-driven nature, and ways in which appropriate cybersecurity should be applied to different types of scientific research without crippling the scientific process by placing overly onerous burdens on scientists and scientists' institutions.

G. Broader Impact

As described in our Broader Impacts report [36], Trusted CI is impacting projects across all seven NSF science directorates and underrepresented groups in cybersecurity. The new activities in this proposal, namely the collaboration with the Quilt and the regional networks and strengthened partnership with Internet2, the cybersecurity research transition to practice program, and the Fellows program, will greatly increase this breadth of impact across the NSF directorates and community. As described in the Broader Impacts of our Results from Prior Support, woven into these and our other activities are and will continue to be outreach to underrepresented populations in cybersecurity. We will use our connections with the following groups to strive for inclusive participation in our Fellows program and workshops: Women in Security and Privacy (WISP) [196], Society of Women Engineers (SWE) [98], National Society of Black Engineers (NSBE), Society for Hispanic Professional Engineers (SHPE) [99], the American Indian Science and Engineering Society (AISES) [197], and the Minority Serving Cyberinfrastructure Consortium (MS-CC) [60]. In aggregate these activities expand and mature the NSF community addressing cybersecurity in support of NSF science, and work to promote reproducible, trustworthy science.

References

1. **“Cybersecurity Innovation for Cyberinfrastructure (CICI) (nsf19514) | NSF - National Science Foundation”** Available at <https://www.nsf.gov/pubs/2019/nsf19514/nsf19514.htm>
2. Welch, V., Basney, J., Jackson, C., Marsteller, J., and Miller, B. **“The Trusted CI Vision for an NSF Cybersecurity Ecosystem And Five-Year Strategic Plan (2019-2023)”** Available at <http://hdl.handle.net/2022/22178>
3. **“Research Areas | NSF - National Science Foundation”** Available at https://www.nsf.gov/about/research_areas.jsp
4. **“NSF’s 10 Big Ideas - Special Report | NSF - National Science Foundation”** Available at https://www.nsf.gov/news/special_reports/big_ideas/
5. **“Home - The Quilt”** *The Quilt* Available at <https://www.thequilt.net/>
6. **“Office of Budget, Finance, and Award Management: Large Facilities Office (LFO) | NSF - National Science Foundation”** Available at <https://www.nsf.gov/bfa/lfo/>
7. **“NSF Big Data Innovation Hubs”** *NSF Big Data Innovation Hubs* Available at <https://www.bigdatahubs.io/>
8. **“Home - Science Gateways Community Institute (SGCI)”** Available at <https://sciencegateways.org/>
9. **“Home: Pilot Study for a Cyberinfrastructure Center of Excellence”** Available at <http://cicoe-pilot.org>
10. **“Home - Engagement and Performance Operations Center (EPOC)”** *Engagement and Performance Operations Center (EPOC)* Available at <https://epoc.global/>
11. Ricker, K., Barlow, J., and Adams, C. **“FBI Major Case 216: A Case Study”** (2008): doi:10.13140/2.1.2775.2644, Available at <https://dx.doi.org/10.13140/2.1.2775.2644>
12. Ramsey, S. **“Anatomy of a Breach: Lessons Learned”** (2015): Available at <http://hdl.handle.net/2022/22122>
13. Perpetch, N. **“How Cyber Attackers Almost Stole a Unique Chance from Australian Astrophysicists”** *ABC News* (2017): Available at <http://www.abc.net.au/news/2017-10-17/cyber-attack-almost-costs-team-look-at-colliding-neutron-stars/9055816>
14. Estes, A. C. **“Anonymous: Still Trolling After All These Years”** *Gizmodo* (2015): Available at <https://gizmodo.com/anonymous-still-trolling-after-all-these-years-1700374189>
15. **“US Researcher Caught Mining for Bitcoins on NSF Iron”** *HPCwire* (2014): Available at <https://www.hpcwire.com/2014/06/09/us-researcher-caught-mining-bitcoins-nsf-iron/>
16. Nakashima, E. **“Research Firm Releases New Details on Alleged Iranian Hacking Campaign Targeting 300 Universities”** *The Washington Post* (2018): Available at

https://www.washingtonpost.com/world/national-security/iranian-hackers-allegedly-stole-sensitive-research-from-300-universities-heres-how/2018/03/26/60717806-310d-11e8-8abc-22a366b72f2d_story.html

17. Subcommittee on Oversight (Committee on Science, Space, and Technology). “**Hearing: Scholars or Spies: Foreign Plots Targeting America’s Research and Development**” *U.S. House of Representatives Committee Repository* (2018): Available at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108175>

18. “**Theft of US R&D by Other Nations Grabs Attention of Science Committee**” (2018): Available at https://www.aip.org/fyi/2018/theft-us-rd-other-nations-grabs-attention-science-committee?utm_medium=email&utm_source=FYI&dm_i=1ZJN,5KYAB,QOU3JK,LOFBW,1

19. NSF Advisory Committee for Cyberinfrastructure. “**CI2030: Future Advanced Cyberinfrastructure**” (2018): Available at https://www.nsf.gov/cise/oac/ci2030/ACCI_CI2030Report_Approved_Pub.pdf

20. “**HPC Security & Compliance Workshop (PEARC18) – Research Computing**” Available at <https://www.rc.ufl.edu/research/events/workshop-pearc18/>

21. “**NSF and Internet2 to Explore Cloud Computing to Accelerate Science Frontiers | NSF - National Science Foundation**” Available at https://nsf.gov/news/news_summ.jsp?cntn_id=297193

22. Marsteller, J., Welch, V., and Starzynski Coddens, A. “**The Report of the 2016 Cybersecurity Summit for Large Facilities and Cyberinfrastructure: Strengthening Trustworthy Science**” (2016): Available at <https://scholarworks.iu.edu/dspace/handle/2022/21161>

23. Jackson, C., Marsteller, J., Starzynski Coddens, A., and Welch, V. “**Report of the 2015 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure**” (2015): Available at <https://scholarworks.iu.edu/dspace/handle/2022/20539>

24. Peisert, S., Welch, V., Adams, A., Bevier, R., Dopheide, M., LeDuc, R., Meunier, P., Schwab, S., and Stocks, K. “**Open Science Cyber Risk Profile (OSCRP)**” (2017): Available at <https://scholarworks.iu.edu/dspace/handle/2022/21259>

25. Russell, S., Jackson, C., Cowles, B., and Avila, K. “**2017 NSF Community Cybersecurity Benchmarking Survey Report**” (2018): Available at <http://hdl.handle.net/2022/22171>

26. Cowles, R. and Jackson, C. “**2016 NSF Community Cybersecurity Benchmarking Survey Report**” (2016): Available at <http://hdl.handle.net/2022/21355>

27. Marsteller, J., Jackson, C., Sons, S., Allar, J., Fleury, T., and Duda, P. “**Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects, v1**” (2014): Available at <https://scholarworks.iu.edu/dspace/handle/2022/20026>

28. Adams, A., Dopheide, J., Krenz, M., Marsteller, J., Welch, V., and Zage, J. “**The Report of the 2018 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure**” (2018):

Available at <https://scholarworks.iu.edu/dspace/handle/2022/22588>

29. Jackson, C., Marsteller, J., and Welch, V. “**Report of the 2014 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure**” (2014): Available at <https://scholarworks.iu.edu/dspace/handle/2022/19244>

30. Jackson, C., Marsteller, J., and Welch, V. “**Report of the 2013 NSF Cybersecurity Summit for Cyberinfrastructure and Large Facilities: Designing Cybersecurity Programs in Support of Science**” (2014): Available at <http://hdl.handle.net/2022/17588>

31. Dooley, R., Edmonds, A., Hancock, D. Y., Lowe, J. M., Skidmore, E., Adams, A. K., Kiser, R., Krenz, M., Welch, V., and Knepper, R. “**Security Best Practices for Academic Cloud Service Providers**” (2018): Available at <http://hdl.handle.net/2022/22123>

32. National Science Foundation. “**Agency Information Collection Activities: Proposed Collection; Comment Request**” *Federal register* 83, (2018): 65757–65759. Available at <https://www.federalregister.gov/documents/2018/12/21/2018-27622/agency-information-collection-activities-proposed-collection-comment-request>

33. “**Trusted CI Training Materials**” *Trusted CI: the NSF Cybersecurity Center of Excellence* Available at <https://trustedci.org/trainingmaterials/>

34. Anderson, S., Deelman, E., Parashar, M., Pascucci, V., Petravick, D., and Rathje, E. M. “**Report from the NSF Large Facilities Cyberinfrastructure Workshop**” (2017): Available at <http://facilitiesci.org/images/facilitiesci-workshop-report-11-17.pdf>

35. Parashar, M. “**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**” (2018): Available at <https://meetings.internet2.edu/2018-global-summit/detail/10004995/>

36. Dopheide, J., Zage, J., and Basney, J. “**The Trusted CI Broader Impacts Project Report (pending)**” (2018): Available at <http://hdl.handle.net/2022/22148>

37. Welch, V. “**Trusted CI - The NSF Cybersecurity Center of Excellence: Year Three Report**” (2018): Available at <https://scholarworks.iu.edu/dspace/handle/2022/22597>

38. Welch, V. “**Center for Trustworthy Scientific Cyberinfrastructure - The NSF Cybersecurity Center of Excellence: Year Two Report**” (2017): Available at <https://scholarworks.iu.edu/dspace/handle/2022/21863>

39. Welch, V. “**Center for Trustworthy Scientific Cyberinfrastructure - The NSF Cybersecurity Center of Excellence: Year One Report**” (2016): Available at <https://scholarworks.iu.edu/dspace/handle/2022/21163>

40. Welch, V. “**Center for Trustworthy Scientific Cyberinfrastructure: Final Report**” (2016): Available at <https://scholarworks.iu.edu/dspace/handle/2022/21073>

41. Welch, V. “**Year Three Report: Center for Trustworthy Scientific Cyberinfrastructure**” (2015): Available at <https://scholarworks.iu.edu/dspace/handle/2022/20401>

42. Welch, V. **“Year Two Report: Center for Trustworthy Scientific Cyberinfrastructure”** (2014): Available at <https://scholarworks.iu.edu/dspace/handle/2022/20030>
43. Welch, V. **“Year 1 Report: Center for Trustworthy Scientific Cyberinfrastructure”** (2013): Available at <https://scholarworks.iu.edu/dspace/handle/2022/17205>
44. **“Trusted CI Webinars”** *Trusted CI: the NSF Cybersecurity Center of Excellence* Available at <https://trustedci.org/webinars/>
45. **“Large Facilities Security Team”** *Trusted CI: the NSF Cybersecurity Center of Excellence* Available at <https://trustedci.org/lfst/>
46. **“Identity and Access Management — Trusted CI: The NSF Cybersecurity Center of Excellence”** *Trusted CI: the NSF Cybersecurity Center of Excellence* Available at <https://trustedci.org/iam/>
47. **“Trusted CI Celebrates Five Years of Trustworthy Science”** *HPCwire* (2018): Available at <https://www.hpcwire.com/2018/05/01/trusted-ci-celebrates-five-years-of-trustworthy-science/>
48. **“Does Security Ruin Efficiency?”** *Science Node* Available at <https://sciencenode.org/feature/security-efficiency.php>
49. **“URISC@SC17 and a Tale of Four Unicorns”** *HPCwire* (2017): Available at <https://www.hpcwire.com/2017/09/08/uriscsc17-tale-four-unicorns/>
50. **“IU Hosts Cybersecurity Workshop to Help Opposites Attract”** *IU hosts cybersecurity workshop to help opposites attract* Available at <https://itnews.iu.edu/articles/2017/iu-hosts-cybersecurity-workshop-to-help-opposites-attract.php>
51. **“What Does Security Mean in Science Today?”** *Science Node* Available at <https://sciencenode.org/feature/what-does-security-mean-in-science-today.php>
52. **“Center for Trustworthy Scientific Cyberinfrastructure to Provide Cybersecurity Services Tailored to NSF Community”** *Scientific Computing* (2016): Available at <https://www.scientificcomputing.com/news/2016/01/center-trustworthy-scientific-cyberinfrastructure-provide-cybersecurity-services>
53. **“NCSA’s Partnership with Trusted CI Helps Secure Over \$7 Billion of Science”** *HPCwire* Available at <https://www.hpcwire.com/off-the-wire/ncsas-partnership-with-trusted-ci-helps-secure-over-7-billion-of-science/>
54. **“Cybersecurity to Enable Science: Hindsight & Vision from the NSF Cybersecurity Center of Excellence | NSF - National Science Foundation”** Available at https://www.nsf.gov/events/event_summ.jsp?cntn_id=296635&org=NSF
55. **“PEARC Conference Series”** *PEARC Conference Series* Available at <https://www.pearc.org/>
56. **“SI2 PI Meeting 2018”** Available at <https://si2-pi-community.github.io/2018-meeting/>

57. **“Annual Conference - Science Gateways Community Institute (SGCI)”** Available at <https://sciencegateways.org/engage/annual-conference>
58. **“STEM-Trek”** Available at <http://www.stem-trek.org/>
59. **“Promoting Cybersecurity for Open Science: CTSC Plays Key Role in URISC Workshop at SC17”** Available at <https://cacr.iu.edu/news/2017/Promoting%20cybersecurity%20for%20open%20science.php>
60. **“SPACI@MSIs | Just Another WordPress Site”** Available at <http://spaci.scsu.edu/>
61. Welch, V. **“The NSF Cybersecurity Center of Excellence: Cybersecurity for Science”** (2016): doi:10.6084/m9.figshare.3118153.v2, Available at <http://dx.doi.org/10.6084/m9.figshare.3118153.v2>
62. Welch, V. **“Cybersecurity for Science”** (2017): doi:10.6084/m9.figshare.5028761.v1, Available at <http://dx.doi.org/10.6084/m9.figshare.5028761.v1>
63. Welch, V. **“Cybersecurity for Open Science”** (2017): doi:10.6084/m9.figshare.5592718.v1, Available at <http://dx.doi.org/10.6084/m9.figshare.5592718.v1>
64. Welch, V. **“Cybersecurity for Research on Small Campuses”** (2018): doi:10.6084/m9.figshare.6667541.v1, Available at <http://dx.doi.org/10.6084/m9.figshare.6667541.v1>
65. **“FY 2018 Budget Request to Congress: List of Tables | NSF - National Science Foundation”** Available at <https://www.nsf.gov/about/budget/fy2018/tables.jsp>
66. **“2016 Federal Cybersecurity Research and Development Strategic Plan”** (2016): Available at <https://www.nitrd.gov/cybersecurity/>
67. Ron Ross, Kelley Dempsey, Patrick Viscuso, Mark Riddle, Gary Guissanie. **“SP 800-171 Rev. 1, Protecting CUI in Nonfederal Systems and Organizations | CSRC”** Available at <https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final>
68. Welch, V. **“Cybersecurity: We Don’t Have It Right Yet”** (2018): doi:10.6084/m9.figshare.7011785.v1, Available at <http://dx.doi.org/10.6084/m9.figshare.7011785.v1>
69. Prepared by the Large Facilities Office in the Budget, Finance, and Award Management Office (BFA-LFO). **“NSF Large Facilities Manual”** (2017): Available at <https://www.nsf.gov/pubs/2017/nsf17066/nsf17066.pdf>
70. **“Carcc.org – Campus Research Computing Consortium”** Available at <https://carcc.org/>
71. **“WISE Community – Wise Information Security for Collaborating E-Infrastructures”** Available at <https://wise-community.org/>
72. **“Gemini Observatory”** *Gemini Observatory* Available at <https://www.gemini.edu/>

73. **"IceCube Neutrino Observatory"** Available at <https://icecube.wisc.edu/>
74. Large Synoptic Survey Telescope. **"Welcome | The Large Synoptic Survey Telescope"** Available at <https://www.lsst.org/>
75. **"Home Page - NSO - National Solar Observatory"** *NSO - National Solar Observatory* Available at <https://www.nso.edu/>
76. **"NEON"** Available at <https://www.neonscience.org/>
77. **"National Energy Research Scientific Computing Center"** Available at <http://www.nersc.gov/>
78. **"Home: Energy Science Network"** Available at <http://es.net/>
79. **"Welcome to NCI - National Computational Infrastructure"** *National Computational Infrastructure* Available at <http://nci.org.au/>
80. Head of School. **"ANU Appoints CEO of Cyber Institute"** *The Australian National University* (2018): Available at <https://eng.anu.edu.au/news/anu-appoints-ceo-cyber-institute>
81. **"Globus Online Ensures Research Data Integrity | Globus"** Available at <https://www.globus.org/blog/globus-online-ensures-research-data-integrity>
82. Welch, V. **"Software Integrity with Pegasus: Securing Scientific Workflow Data"** (2018): doi:10.6084/m9.figshare.7430252.v1, Available at https://figshare.com/articles/Software_Integrity_with_Pegasus_Securing_Scientific_Workflow_Data/7430252
83. Bernd Panzer-Steindel, C. **"Data Integrity"** Available at https://indico.cern.ch/event/13797/contributions/1362288/attachments/115080/163419/Data_integrity_v3.pdf
84. **"User News - XSEDE"** Available at <https://www.xsede.org/news/user-news/-/news/item/6390>
85. Paxon, V. **"End-to-End Internet Packet Dynamics"** *IEEE/ACM Transactions on Networking* 7, no. 3 (1999): 277–292.
86. **"Data Management and Information Governance"** *Ostrom Workshop* Available at <https://ostromworkshop.indiana.edu/research/data-management/index.html>
87. **"Indiana Geological and Water Survey"** Available at <https://igws.indiana.edu/>
88. **"Array of Things"** Available at <https://arrayofthings.github.io/>
89. **"DesignSafe | DesignSafe-CI"** Available at <https://www.designsafe-ci.org/>
90. **"National Science Foundation FY 2017 Performance and Financial Highlights (nsf18021)"** Available at <https://www.nsf.gov/pubs/2018/nsf18021/nsf18021.pdf>
91. **"CC-NIE Peer Review — Trusted CI: The NSF Cybersecurity Center of Excellence"**

Trusted CI: the NSF Cybersecurity Center of Excellence Available at <https://trustedci.org/cc-nie>

92. **“Webinar: Authorizing Access to Science Gateway Resources - Webinar Detail - Science Gateways Community Institute (SGCI)”** Available at <https://sciencegateways.org/-/authorizing-access-to-science-gateway-resources?inheritRedirect=true&redirect=%2Fengage%2Fwebinar-archive>

93. **“Fellowship Programme | Software Sustainability Institute”** Available at <https://www.software.ac.uk/fellowship-programme>

94. **“Trusted CI Advisory Committee”** *Trusted CI: the NSF Cybersecurity Center of Excellence* Available at <https://trustedci.org/advisory-committee/>

95. **“Campus Champions - XSEDE”** Available at <https://www.xsede.org/community-engagement/campus-champions>

96. **“Established Program to Stimulate Competitive Research (EPSCoR) | National Science Foundation”** Available at <https://www.nsf.gov/od/oia/programs/epscor/>

97. **“Coalition for Academic Scientific Computation”** Available at <http://casc.org/>

98. **“Home | Society of Women Engineers”** Available at <http://societyofwomenengineers.swe.org/>

99. **“Society of Hispanic Professional Engineers - Welcome”** Available at <http://www.shpe.org/>

100. **“Diversity and Inclusion - XSEDE”** Available at <https://www.xsede.org/community-engagement/diversity>

101. **“HPCwire: Global News and Information on High Performance Computing (HPC)”** *HPCwire* Available at <https://www.hpcwire.com/>

102. **“Science Node”** Available at <https://sciencenode.org/>

103. **“Cybersecurity at IUB: News Archive: News: Center of Excellence for Women in Technology (CEWiT): Indiana University Bloomington”** Available at <http://cewit.indiana.edu/news/archive/Meet-IUB-Cybersecurity-Women.shtml>

104. **“Video Conferencing, Web Conferencing, Webinars, Screen Sharing”** *Zoom Video* Available at <https://zoom.us/>

105. Marsteller, J., Russell, S., and Welch, V. **“The Report of the 2017 Cybersecurity Summit for Large Facilities and Cyberinfrastructure”** (2018): Available at <http://hdl.handle.net/2022/21882>

106. Welch, V. **“An Overview of CTSC Engagements & Application Process”** (2017): Available at <https://scholarworks.iu.edu/dspace/handle/2022/21640>

107. **“Welcome to the DKIST | DKIST”** Available at <https://dkist.nso.edu/>

108. **"Ocean Observatories Initiative"** *Ocean Observatories Initiative* Available at <http://oceanobservatories.org/>
109. Marsteller, J. **"Large Synoptic Survey Telescope (LSST) Realigns Cybersecurity Plan to CTSC's Guide"** Available at <http://blog.trustedci.org/2015/06/large-synoptic-survey-telescope-lsst.html>
110. **"Home - LTER"** *LTER* Available at <https://lternet.edu/>
111. **"University of New Hampshire Research Computing Center"** *UNH Research Office* (2018): Available at <https://www.unh.edu/research/research-computing-center>
112. **"TransPAC"** Available at <https://internationalnetworks.iu.edu/initiatives/transpac/>
113. **"HUBzero"** *HUBzero* Available at <https://hubzero.org/>
114. **"National Radio Astronomy Observatory - National Radio Astronomy Observatory"** *National Radio Astronomy Observatory* Available at <https://public.nrao.edu/>
115. **"The USAP Portal: Science and Support in Antarctica - Welcome to the United States Antarctic Program Portal"** Available at <https://www.usap.gov/>
116. **"Home [CyberGIS]"** (2016): Available at <http://cybergis.cigi.uiuc.edu/>
117. Zage, J. **"CPP-CTSC SFS Cyberinfrastructure Security Workshop"** Available at <http://blog.trustedci.org/2017/12/cal-poly-blog-post-on-weekend-of.html>
118. **"Agave Platform"** *Agave Platform* Available at <https://agaveapi.co/>
119. **"CyVerse | Cyberinfrastructure for Data Management and Analysis"** *CyVerse | Cyberinfrastructure for Data Management and Analysis* Available at <http://www.cyverse.org/>
120. **"Jetstream: A National Science and Engineering Cloud"** Available at <https://jetstream-cloud.org/>
121. **"GenApp Framework"** Available at <https://genapp.rocks/>
122. **"Open Science Grid"** Available at <https://www.opensciencegrid.org/>
123. **"Research Data Management Simplified. | Globus"** Available at <https://www.globus.org/>
124. **"DataONE"** Available at <https://www.dataone.org/>
125. **"LSC - LIGO Scientific Collaboration"** Available at <https://www.ligo.org/>
126. OSIRIS Project. **"OSIRIS"** Available at <http://www.osiris.org/>
127. **"SciGaP"** Available at <https://scigap.org/>
128. **"Wildbook: Software to Combat Extinction"** Available at <http://wildbook.org/doku.php>

129. “**perfSONAR Home | perfSONAR**” Available at <https://www.perfsonar.net/>
130. “**Engagement Application — Trusted CI: The NSF Cybersecurity Center of Excellence**” *Trusted CI: the NSF Cybersecurity Center of Excellence* Available at <https://trustedci.org/application/>
131. “**Minority Serving Institutions Program**” (2015): Available at <https://www.doi.gov/pmb/eeo/doi-minority-serving-institutions-program>
132. “**Trusted CI: The NSF Cybersecurity Center of Excellence**” *Trusted CI: the NSF Cybersecurity Center of Excellence* Available at <https://trustedci.org/>
133. “**Trusted CI Blog**” Available at <http://blog.trustedci.org/>
134. “**Trusted CI Email Lists**” Available at <https://trustedci.org/ctsc-email-lists/>
135. “**Trusted CI Twitter Feed**” Available at <https://twitter.com/trustedci>
136. “**Trusted CI - YouTube**” Available at <https://www.youtube.com/channel/UCD2sZ957eokDw8mcjkHXvXw>
137. “**Trusted CI Presentations**” *Trusted CI: the NSF Cybersecurity Center of Excellence* Available at <https://trustedci.org/presentations/>
138. Trusted CI. “**Trusted CI Webinar: The EU General Data Protection Regulation (GDPR)**” (2018): Available at <https://www.youtube.com/watch?v=Lr37InxEbbc&feature=youtu.be>
139. “**Meltdown and Spectre**” Available at <https://meltdownattack.com/>
140. “**Mid-Scale Research Infrastructure-2 | NSF - National Science Foundation**” Available at https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=505550&org=OAC&from=home
141. Slack. “**Where Work Happens**” *Slack* Available at <https://slack.com/>
142. “**Cyberinfrastructure Vulnerabilities**” *Trusted CI: the NSF Cybersecurity Center of Excellence* Available at <https://trustedci.org/vulnerabilities/>
143. “**Home - XSEDE**” Available at <https://www.xsede.org/>
144. “**Cyberinfrastructure: From Supercomputing to the TeraGrid | NSF - National Science Foundation**” Available at https://www.nsf.gov/news/special_reports/cyber/fromsctotg.jsp
145. “**Traffic Light Protocol (TLP) Definitions and Usage | US-CERT**” Available at <https://www.us-cert.gov/tlp>
146. “**Research Security Operations Center (ResearchSOC)**” *Research Security Operations Center (ResearchSOC)* Available at <https://researchsoc.iu.edu/>
147. Blogger, G. “**Helping Scientists Understand Research Cyber Risks**” *UC IT Blog* Available at <https://cio.ucop.edu/helping-scientists-understand-research-cyber-risks/>
148. Peisert, S. and Welch, V. “**The Open Science Cyber Risk Profile: The Rosetta Stone for**

Open Science and Cybersecurity” *IEEE Security & Privacy* no. 5 (2017): 94–95.
doi:10.1109/MSP.2017.3681058, Available at
<https://www.computer.org/csdl/mags/sp/2017/05/msp2017050094-abs.html>

149. **“Mind the Gap: Speaking like a Cybersecurity pro”** *Science Node* Available at
<https://sciencenode.org/feature/mind-the-gap-how-to-speak-like-an-information-security-pro.php>

150. **“OSCRP”** Available at <https://github.com/trustedci/OSCRP>

151. **“Energy Sciences Network (ESnet)”** Available at <https://www.es.net/>

152. Sons, S. **“NSF Cybersecurity Center of Excellence, ESnet Organize Working Group on Open Science Threats”** (2016): Available at
<http://blog.trustedci.org/2016/06/nsf-cybersecurity-center-of-excellence.html>

153. **“nsf18547 Cybersecurity Innovation for Cyberinfrastructure (CICI)”** *National Science Foundation* (2018): Available at
https://www.nsf.gov/publications/pub_summ.jsp?ods_key=nsf18547

154. Welch, V. **“Open Science Cyber Risk Profile Publications”** Available at
<http://blog.trustedci.org/2017/10/open-science-cyber-risk-profile.html>

155. **“Software Assurance Marketplace”** *Welcome to the SWAMP, the Software Assurance Marketplace*. Available at <https://continuousassurance.org/>

156. **“Principles-Based Assessment for Cybersecurity Toolkit”** Available at
<https://cacr.iu.edu/pact/>

157. **“Home | Internet2”** Available at <https://www.internet2.edu/>

158. **“Communities & Groups | Internet2”** Available at
<https://www.internet2.edu/communities-groups/members/higher-education/all/all/all>

159. Dart, E., Rotman, L., Tierney, B., Hester, M., and Zurawski, J. **“The Science DMZ: A Network Design Pattern for Data-Intensive Science”** *SC '13: Proceedings of the International Conference on High Performance Computing, Networking, Storage and Analysis* (2013): 1–10.
doi:10.1145/2503210.2503245, Available at <http://dx.doi.org/10.1145/2503210.2503245>

160. **“Home | 2019 Internet2 Global Summit”** Available at
<https://meetings.internet2.edu/2019-global-summit/>

161. **“What Do Research Computing and Information Security Leaders Have in Common? | Internet2 Blogs”** Available at <https://www.internet2.edu/blogs/detail/16960>

162. **“CyberCorps(R) Scholarship for Service | NSF - National Science Foundation”**
Available at https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504991&org=NSF

163. Executive Office of the President and National Science and Technology Council. **“Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program”** (2011): Available at

<https://www.nitrd.gov/Publications/PublicationDetail.aspx?pubid=39>

164. Dopheide, J. "**CCoE Webinar May 22nd 11am ET: Cybersecurity Research: Transition To Practice (TTP)**" (2017): Available at

<https://blog.trustedci.org/2017/05/ccoe-webinar-may-22nd-11am-et.html>

165. "**Secure and Trustworthy Cyberspace (SaTC)**" Available at

<http://www.nsf.gov/pubs/2016/nsf16580/nsf16580.htm>

166. "**Partnerships for Innovation | NSF - National Science Foundation**" Available at

https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504790

167. "**I-Corps - NSF - National Science Foundation**" Available at

https://www.nsf.gov/news/special_reports/i-corps/

168. "**NSF SBIR | NSF SBIR**" Available at <https://seedfund.nsf.gov/>

169. "**2017 Technology Exchange - CINC UP: Cybersecurity Research Acceleration Workshop and Showcase - CINO Working Groups - Internet2 Wiki**" Available at

<https://spaces.internet2.edu/display/CWG/2017+Technology+Exchange+-+CINC+UP%3A+Cybersecurity+Research+Acceleration+Workshop+and+Showcase>

170. "**Global Summit 2017 - CINC UP: Cybersecurity Research Acceleration Workshop & Showcase - CINO Working Groups - Internet2 Wiki**" Available at

<https://spaces.internet2.edu/pages/viewpage.action?pageId=115179609>

171. "**Bunker Labs**" Available at <https://bunkerlabs.org/>

172. "**SWE Chicago Regional Section**" *SWE Chicago Regional Section* Available at

<http://chicago.swe.org/>

173. "**SHPE Chicago – Society of Hispanic Professional Engineers**" Available at

<https://shpechicago.org/>

174. "**NSBE Chicago**" *mysite* Available at <https://www.chicagonsbe.org/>

175. Simpkins, J. "**Women in Technology: Cyber Security & Technology Special Interest Group (Cyber & Tech SIG)**" Available at

<https://www.womenintechnology.org/cyber-security-technology-sig>

176. "**Cybersecurity Technology Transfer to Practice (TTP)**" Available at

<https://www.southalabama.edu/colleges/soc/research/ttp/>

177. "**CSD-TTP**" *Department of Homeland Security* (2013): Available at

<https://www.dhs.gov/science-and-technology/csd-ttp>

178. Short, H. "**WISE@NSF Summit – WISE Community**" Available at

<https://wise-community.org/2017/07/19/wisensf-summit/>

179. "**WISE @ NSF CyberSecurity Summit 2018 - WISE - GÉANT Federated Confluence**"

Available at <https://wiki.geant.org/display/WISE/WISE+@+NSF+CyberSecurity+Summit+2018>

180. **"The Zeek Network Security Monitor"** Available at <https://www.zeek.org/>

181. Dopheide, J. **"Student Program at the 2018 NSF Cybersecurity Summit"** Available at <https://blog.trustedci.org/2018/09/student-program-at-2018-nsf.html>

182. **"Dear Colleague Letter: Software Infrastructure for Sustained Innovation (SI2) Program in Fall 2017"** (2017): Available at <https://www.nsf.gov/pubs/2017/nsf17126/nsf17126.jsp>

183. **"The SC Conference Series"** Available at <http://supercomputing.org/>

184. **"Trusted CI: Software Assurance"** *Trusted CI: the NSF Cybersecurity Center of Excellence* Available at <https://trustedci.org/software-assurance/>

185. Kupsch, J. A., Miller, B. P., Heymann, E., and César, E. **"First Principles Vulnerability Assessment"** *Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop* (2010): 87–92. doi:10.1145/1866835.1866852, Available at <http://doi.acm.org/10.1145/1866835.1866852>

186. **"Trusted CI Reports"** *Trusted CI: the NSF Cybersecurity Center of Excellence* Available at <https://trustedci.org/reports/>

187. **"CILogon"** Available at <http://www.cilogon.org/>

188. Withers, A., Bockelman, B., Weitzel, D., Brown, D., Gaynor, J., Basney, J., Tannenbaum, T., and Miller, Z. **"SciTokens: Capability-Based Secure Access to Remote Scientific Data"** *Proceedings of the Practice and Experience on Advanced Research Computing* (2018): 24. doi:10.1145/3219104.3219135, Available at <https://dl.acm.org/citation.cfm?doid=3219104.3219135>

189. **"ImPACT | RENCI"** Available at <http://renci.org/impact/>

190. **"NSF Award Search: Award#1840003 - CICI: SSC: Securing Science Gateway Cyberinfrastructure with Custos"** Available at https://www.nsf.gov/awardsearch/showAward?AWD_ID=1840003

191. **"NSF Award Search: Award#1827641 - PFI-TT: Using Science Gateways to Enable Greater Access to High Performance Computing in Support of Advanced Manufacturing"** Available at https://www.nsf.gov/awardsearch/showAward?AWD_ID=1827641&HistoricalAwards=false

192. Wickman, G. **"Traction: Get a Grip on Your Business"** (2012): Available at https://books.google.com/books/about/Traction.html?id=1sl__J9p70AC

193. **"Google Docs - Create and Edit Documents Online, for Free"** Available at <https://www.google.com/docs/about/>

194. **"GitHub: Trusted CI"** Available at <https://github.com/trustedci>

195. **“Trusted CI’s Cybersecurity Program”** *Trusted CI: the NSF Cybersecurity Center of Excellence* Available at <https://trustedci.org/cybersecurity-program/>

196. **“Women in Security and Privacy”** *Women in Security and Privacy* Available at <https://www.wisporg.com/>

197. **“American Indian Science and Engineering Society (AISES)”** *AISES* Available at <http://www.aises.org/>

CICI: CCoE: Trusted CI: Advancing Trustworthy Science

Data Management Plan

Description of data to be generated in this project:

During the course of the proposed project, data generated that should persist will be training materials and other public documentation (e.g., best practice guides, lessons learned educational curriculum, engagement reports). Trusted CI does not expect to generate or capture experimental or other data that would necessitate a relational database or specific data file formats for programmatic access from computer models. We expect that all of the data generated by this project can be projected into the Adobe Portable Document Format (PDF), and preserved as described below. PDF documents are commonly full text indexed by search engines, and are available to text mining and natural language processing systems. The project team expects that the ability to consume and manage content in the PDF file format will outlive the meaningfulness of the data generated by Trusted CI.

The project will generate some data, related to its work in software assessment and engagement activities, which will not be immediately public until we have had a chance to work with involved parties to perform responsible disclosure, after which time the data will become public. The PIs are familiar with this process and our cybersecurity plan includes our processes for handling this sort of sensitive data.

Responsibility for data management:

Ultimate responsibility for data management within Trusted CI will reside with PI Von Welch; however, Trusted CI team members will each be responsible for the management of data within activities they lead. This responsibility includes ensuring that the materials have appropriate search terms and metadata; have project, grant, and partner attribution; have the Trusted CI license declaration; have been cataloged as a project artifact and preserved according to the policies within this data management plan.

License for data generated as a result of this project:

All materials *de novo* generated as part of this project that will be distributed will be distributed under the Creative Commons Attribution-NonCommercial 3.0 Unported (CC BY-NC 3.0). The full terms of this license are available at <http://creativecommons.org/licenses/by-nc/3.0/>. This license includes the following terms: You are free to share – to copy, distribute and transmit the work and to remix – to adapt the work under the following conditions: attribution – you must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work). For any reuse or distribution, you must make clear to others the license terms of this work.

Data preservation, dissemination, and public use:

Trusted CI will leverage the Indiana University ScholarWorks system (<http://scholarworks.iu.edu/>) for data preservation. IU ScholarWorks is a set of services from the Indiana University Libraries and Indiana University Digital Library Program to make the work of IU scholars freely available and ensures that these resources are preserved and organized for the future. Trusted CI will also make its products available on the center's public website, and will take steps to ensure the NSF community and public are aware of these products.

CICI: CCoE: Trusted CI: Advancing Trustworthy Science
Project Personnel and Partner Organizations

1. Stanley C. Ahalt; South Big Data Hub; Collaborator
2. Srinivas Aluru; South Big Data Hub; Collaborator
3. Steve Barnett; IceCube Neutrino Observatory; Collaborator
4. Tom Barton; University of Chicago; Collaborator
5. Jim Basney, University of Illinois Urbana-Champaign; Co-PI
6. Rene Baston; Northeast Big Data Hub; Collaborator
7. Dana Brunson; Internet2; Senior Personnel
8. Tom Cheatem; University of Utah; Collaborator
9. Marianne Chitwood; iLight; Collaborator
10. Neil Chue Hong; UK Software Sustainability Institute (SSI); Collaborator
11. Samuel S. Conn; NJEDGE; Collaborator
12. Robert (Bob) Cowles; Brightlite Information Security; Paid Consultant
13. Melissa Cragin; Midwest Big Data Hub; Collaborator
14. Eric Cross; National Solar Observatory; Collaborator
15. Ewa Deelman; Cyberinfrastructure Center of Excellence Pilot; Collaborator
16. James Deeton; Great Plains Network; Collaborator
17. Brent Draney; NERSC, Collaborator
18. Dr. Ben Evans ; Australian National Computation Institute; Collaborator
19. Kenneth Goodwin; 3ROX; Collaborator
20. Elisa Heiman, University of Wisconsin-Madison; Senior Personnel
21. Florence Hudson, Independent Consultant; Paid Consultant
22. Tim Hudson; National Ecological Observatory Network; Collaborator
23. Wendy Huntoon; KINBER; Collaborator
24. Prof. Mohammad Husain; Cal Poly Pomona; Collaborator
25. Stephen Craig Jackson Jr.; Indiana University; Senior Personnel
26. Steve Kankus; NYSERNet; Collaborator
27. David Kelsey; WISE Community; Collaborator
28. Mark Krenz; Indiana University; Senior Personnel
29. Jen Leasure; The Quilt; Collaborator
30. Meredith Lee; West Big Data Hub; Collaborator
31. Lonnie Leger; LONI; Collaborator
32. Patty Leslie; Front Range GigaPOP, University Corporation for Atmospheric Research; Collaborator
33. David Marble; NEREN and OSHEAN; Collaborator
34. Jim Marsteller; Carnegie Mellon University; Co-PI
35. Dr. Ashwin Mathew; University of California-Berkeley
36. Bart Miller; University of Wisconsin-Madison; Co-PI
37. Chris Morrison; Gemini Observatory; Collaborator
38. Gary Motz; Indiana Geological and Water Survey; Collaborator
39. Nicholas J. Multari; Pacific Northwest National Lab (PNNL); Collaborator
40. Sean Peisert; Lawrence Berkley; Senior Personnel

41. Angie Raymond; Ostrom Data Initiative; Collaborator
42. Jennifer Schopf ; Engagement and Performance Operations Center (EPOC); Collaborator
43. Dr. Lesley Seebeck; Australian National University Cyber Institute, Collaborator
44. Adam Slagell; ESNNet, Collaborator
45. Dr. Mary Stewart; WVNET; Collaborator
46. John Towns; XSEDE; Collaborator
47. Professor Steven Weber; University of California-Berkeley
48. Nancy Wilkins-Diehr; San Diego Supercomputing Center and NSF Science Gateway Community Institute (SGCI); Collaborator
49. Alexander Withers; Large Synoptic Survey Telescope (LSST); Collaborator
50. Melissa Woo; Stony Brook University; Collaborator
51. Dr. Alec Yasinsac; The University of South Alabama; Collaborator

CICI: CCoE: Trusted CI: Advancing Trustworthy Science

Project Plan Supplemental Document

Goals and Milestones

Trusted CI's goal is to enable productive, reproducible, trustworthy science by leading "in the development of an NSF Cybersecurity Ecosystem with the workforce, knowledge, processes, and cyberinfrastructure that enables trustworthy science and the NSF's vision of a nation that is a global leader in research and innovation." This goal is challenging to measure directly, so while we track anecdotes that mark our success in achieving it, we use the following proxy metrics as discussed in section D.13 of our proposal:

- Adoption of cybersecurity programs by members of the NSF community as measured by our Community Benchmark Survey (<http://hdl.handle.net/2022/22171>).
- The breadth of our impact across the NSF community as captured in our Broader Impacts Project Report (<http://hdl.handle.net/2022/22148>) and in future Annual Reports to NSF.

Milestones

Key to the success of Trusted CI is to provide the community with stable, reliable services. This means that many of our services are operational in nature and, barring some factor that leads the management team to believe change is warranted, will similar milestones from year-to-year. Hence, we provide milestones in a mixture of quarterly milestones that we expect to be repetitive from year-to-year, and annual milestones showing how an activity will evolve over the course of the five years. Following the milestones, Figures 1 and 2 show our internal management mechanisms to allocated resources to milestones and track progress.

- Section D.1: Providing Leadership for Cybersecurity for Science
 - Trusted CI Framework: An Architecture for Cybersecurity Programs
 - The Framework is a leadership activity and its timeline will be very responsive to the response and feedback from the community. Our expectation for its evolution over the five years is:
 - Year 1: Draft available, based on work in 2019 under current funding.
 - Year 2: Goal: three members of the community, NSF projects and research computing centers, adopting the framework
 - Year 3: Revision of Framework based on initial communities experiences. Goal: five more community members, including one with international interoperability needs (Europe or Australia most likely).
 - Years 4 and year 5: Goal: Five more members of community adopting each year.
 - Ongoing activity: Track updates to the NSF Major Facilities Guide and provide feedback and make changes to keep it and the Framework compatible.
 - Annual Challenge:
 - Each year our topic will be new, but our basic process will be similar, barring improvements as we learn as we go along.
 - Quarter 1: Convene collaborative team, agreeing on specific details of the challenge and the needed analysis, begin surveying and gathering community input and requirements.

- Quarter 3:
 - Commence engagements arranged during the prior quarter.
 - Plan engagement application for following year.
 - Quarter 4:
 - Complete engagements and provide reports to engaged projects (and publish if they are amenable).
 - Select engagements for following year through open application process.
- Section D.4: Ongoing Outreach: Webinars, Office Hours, Social Media, Training
 - Large Facilities Security Team (LFST): We hold a monthly meeting, with topics as requested by the LFST or suggested by the Trusted CI team. We convene this group in person at the NSF Cybersecurity Summit in Q4.
 - Webinars: Held monthly with an annual call for presenters.
 - YouTube: Archive webinars to YouTube.
 - Website: Update monthly with upcoming events and review for outdated materials.
 - Blog, Twitter, email lists: Advertise our events, news, new resources, third party news of interest to the community as appropriate.
 - Presentations: We regularly present at the Internet2 Global Summit, EDUCAUSE Security Professionals Conference, PEARC, and the NSF Cybersecurity Summit. We constantly seek out other opportunities to present (e.g. NSF PI meetings, project meetings, the NSF Large Facilities CI workshop).
 - Training: In Q1, we plan what training needs to be updated or developed for the NSF Cybersecurity Summit, PEARC, and other venues, and schedule that work through the year.
- Section D.5: Situational Awareness for Improved Risk Management
 - Ongoing: We monitor information sources and select what vulnerabilities to pass onto the community, with our added guidance.
 - Ongoing: We seek out new partners (joining us, the ResearchSOC, XSEDE, and the Open Science Grid) to collaborate with on this service.
 - Quarterly: We author a blog post with a list of vulnerabilities from the service as advertisement to the community.
- Section D.6. Coordination with the ResearchSOC for Efficient and Effective Cybersecurity
 - This is an ongoing activity that the leadership team will review quarterly at its quarterly strategy meeting described in Section E.
- Section D.7. Refining the Science Threat Model and Countermeasures
 - The Open Science Cyber Risk Profile (OSCRP) is a living document we will evolve continuously over the life of our project through a mixture of ongoing and annual activities:
 - Ongoing: Accept community contributions, vet, and add to the OSCRP.
 - Quarter 1: Select focus area for Trusted CI efforts during Quarters 2 and 3. Invite and convene a working group of experts in those areas to contribute.
 - Quarters 2 and 3: Lead working group in making contributions to OSCRP.
 - Quarter 4: Review results of NSF Cybersecurity Summit and Annual Challenge for contributions to the OSCRP and incorporate those.
- Section D.8. Interoperability in a Global Science Community
 - Maintenance of these relationships is an ongoing activity and part of other activities as described. In general, we will invite these partners to the annual NSF Cybersecurity Summit (Section D.11) to continuously strengthen the relationship.
- Section D.9. Leveraging the Higher Education Community to Support Trustworthy Science
 - Training to Regional networks in collaboration with the Quilt

- Ongoing: Respond to support requests and questions from the regional networks and their members.
 - Quarter 1-3: In Year One, we will be distilling the training to be provided based on our existing training. We will develop some additional training for the regional networks in how to deliver the training and contact us for support. In subsequent years, we will be updated the training based on feedback from the regional networks and their membership.
 - Quarter 2: In Year Two and beyond, advertise the upcoming training at the Quilt meeting and enroll the cohort to be trained (this cohort is already in place for year one).
 - Quarter 3: Present the Quilt meeting and provide training materials to the regional networks in attendance.
 - Quarter 4: Solicit feedback from the regional networks on the tracking and plan adjustments for the following year.
- Section D.10. Cybersecurity Research Transition to Practice (TTP)
 - Ongoing: Review NSF awards for research that seems ready for transition. Review results of Trusted CI engagements and Annual Challenges to identify NSF project cybersecurity gaps that could be filled with research.
 - Quarter 1: Plan annual workshop by selecting location, venue, and start invitation process.
 - Quarter 2: Host workshop and follow up with researchers and practitioners that seem to be well matched.
 - Quarter 4
 - Follow up with connected researchers and practitioners to gauge success.
 - Host a round table or similar event at the NSF Cybersecurity Summit (Section D.11) to gather needs of the NSF community
- Section D.11. Community Building through the Annual Cybersecurity Summits
 - Quarter 1:
 - Convene program committee and discuss theme(s) for summit.
 - Quarter 2:
 - With program committee, select and invite keynote speaker(s).
 - Publish call for participation
 - Quarter 3:
 - With program committee, select proposed presentation, tutorials, and students.
 - Finalize and publish agenda for summit with as much lead time as possible.
 - Open registration.
 - Open call for host institution for the following year.
 - Quarter 4:
 - Host summit
 - Select venue for following year and contract with venue.
 - Publish report from current year's summit.
- Section D.12. A Solid Foundation for Cyberinfrastructure: Software Assurance
 - Ongoing:
 - Perform two in-depth reviews each year, one each half of the year, as part of Trusted CI's engagement process.
 - Develop new training modules each year and present at the NSF Cybersecurity Summit, PEARC, SC, and other venues as opportunity arises.
- Section D.13. Measuring our Impact on Science
 - In 2021 and 2023 we will conduct our Community Benchmarking Survey by advertising the survey to the community through our outreach channels (Section D.4). Analysis of the

results and developing a draft report takes a quarter. The report is then proofread by the leadership team and published.

- Annually, as part of our annual report writing process in Q4, we will update the impact metrics from our Broader Impact report and include these in our annual report to NSF.
- Metrics for individual activities are included in each quarterly report to NSF.
- Section E: Management
 - Ongoing:
 - Weekly leadership team meetings to review project status and plan for upcoming events.
 - Monthly Trusted CI holds an all-staff meeting to debrief completed activities and share experiences.
 - Quarterly the leadership team holds a two-hour strategy meeting to gauge process on annual goals and make appropriate adjustments.
 - Individual projects and Engagements within Trusted CI hold meetings as appropriate.
 - Individual projects and Engagements report monthly to the leadership team via the Activity Dashboard (see Figure 1) on their status against their project plans. The Leadership Team reviews these activities and makes any needed adjustments if activities are at risk.
 - Quarter 1:
 - Initiate Engagements and other activities as planned the prior quarter.
 - Write quarterly report to NSF and the advisory committee.
 - Review our own cybersecurity plan and make any needed updates. In year two, we will align our cybersecurity plan with the new Trusted CI Framework.
 - Quarter 2:
 - Undertake effort allocation process (see Figure 2) for next six months.
 - Write quarterly report to NSF and the advisory committee.
 - Annual all-staff in-person meeting to reflect on current activities and plan strategy for following year.
 - Quarter 3:
 - Initiate Engagement and other activities as planned the prior quarter.
 - Write quarterly report to NSF and the advisory committee.
 - Quarter 4:
 - Undertake effort allocation process (see Figure 2) for next six months.
 - Write annual report to NSF and the advisory committee.
 - Convene Advisory Committee, typically co-located with the SuperComputing conference.

Project	New Status	Phase	Lead & Members	Leadership POC	Link to Plan	Important Future Dates	Month	December 2018
American Museum of Natural History	Active	Engagement Planning Phase	Henry, Daphne, Zige	Seane	Link	Initial meeting Jan 7	Green	Engagement begins in January.
Zoe Sigmund Center	Active	Engagement Application Phase	Kian, Adams	Walt	Link		Green	Target: EP agreement signoff and engagement start in January.
Redwood Series	Active		Daphne	Seane	Link	Webinars are held the 4th Monday of the month	Green	December 10th webinar: Cloud Security Best Practices with Ron Dosty. 23 non-Trusted CI registered, 16 attended. 7 spent the last couple months looking the 2019 calendar.
Situational Awareness	Active		Adams, Seane, Henry	Seane	Link	Ongoing	Green	Transition from Trusted CI to ResearchDOC is still in progress. Tally will continue with new team after new procedures are established.
Environmental Data Initiative Expansion	Active	Engagement Execution Phase	Henry, Daphne, Zige	Seane	Link	2019-01-27 Contact Mark Serrillo to see if additional project funding was obtained.	Green	The final report was reviewed and approved. We worked on the wrap up blog, including an additional blog highlighting the tutorials from the Engagement. New Major Facilities Guide draft was published to Fed Reg for public comment in late December. First glance shows that it is okay. Bob and Craig

Figure 1: A portion of Trusted CI's Activity Dashboard. Each month activity leaders report to the Leadership Team, giving textual update and status: green – activity on track, yellow – activity at risk of falling behind schedule, or red – activity is behind schedule.

2H2018	Key	Overview	Engagements	Community Services						
Team Member	Trusted CI Allocation (1.0 = 100% FTE, 0.5 = 50% FTE)	Total effort (Automatically calculated. Multiply by 1000 to get total hours)	Environmental Data Initiative	Open to General	SAGE	Budget	Science Gateway Community Institute	Large Facilities & L707	Situational Awareness	Community Benchmarking Survey
Bob C.	0.3	0.2375				0.075				
Craig J.	0.2	0.4375				0.0125		0.0125		0.00625
Leslie B.	0	0.1								
Mark K.	0.4	0.68					0.25			
Scott R.	0.25	0.2125								0.0125
Susan B.	0.2	0.225								
Zaki B.	0.2	0.225								
Van W.	0.3	0.275						0		
Grayson H.	0.25	0.075								
Ryan Kiser	0.3	0.225			0.2					
Diana Borecky	0.15	0.125								
Florence Hudson	0.1									
Arung Shankar	0.2									
Jeanette D.	0.8	0.625		0.1						
Jim B.	0.25	0.225		0.025						0

Figure 2: A portion of a Trusted CI Effort Allocation spreadsheet. Each six months, the leadership puts selected Engagements and activities into columns, and maps effort from rows representing team members to those activities to ensure resources are effectively used but not overcommitted (and hence a risk of work not be completed).

Community Cybersecurity Challenges

Fundamental challenges exist to having cybersecurity that is broadly adopted and effectively support science:

- 1. An effective cybersecurity framework for science must exist.** Cybersecurity today does not address the NSF community challenges stemming from its open environment, distributed collaborations, high-performance infrastructure, flexibility to handle the heterogeneity of the NSF community, and strong need for data integrity. Trusted CI will develop such a capability through its Framework and Annual Challenges (Section D.1).
- 2. The NSF community must be motivated to implement cybersecurity.** Cybersecurity is often seen as a barrier rather than benefit to science productivity. Even with the creation of an effective program, this perception must be overcome. Trusted CI will provide this socialization through our Engagements (Section D.3), our outreach (Section D.4), and Cybersecurity Summits (Section D.11).
- 3. The broader community must accept a science cybersecurity framework as a reasonable complement to other cybersecurity programs.** NSF projects are typically part of universities or other institutions, and have to interoperate with a wide variety of other agencies and countries. To allow for interoperability and stem pressure to adopt less suitable cybersecurity programs, Trusted CI's Framework must be accepted by the broader community. Trusted CI will accomplish this by working with a large set of collaborators from the broader community (Section D.8) and with the higher education information security community (Section D.9).
- 4. The NSF community must be empowered to implement appropriate cybersecurity.** Many NSF projects, especially smaller ones, will need assistance to implement a cybersecurity program. Trusted CI will empower NSF projects of all size and cybersecurity acumen through training, both provided directly (Section D.4) as well as scaled through the regional networks (Section D.9). This will be supported with interactive assistance through email lists and "office hours" (Section D.4),

These challenges impact small projects, multi-institution collaborations, international collaborations, and large facilities, though to different degrees. Small projects will generally be in greater need of training. Multi-institutional and International collaborations will have greater need for broader community acceptance of their cybersecurity program. Large facilities, with stronger management hierarchies, will need more formal presentations and materials to educate and persuade their management of the benefit of cybersecurity programs.

Year One Engagements

We are engaging with the following projects in year one. Section numbers refer to the relevant section of our narrative. Additionally we will hold two open applications for engagements (in late 2019 and then early 2020) to engage with four-to-six more projects based on their specific needs (Section D.3).

- NSF Large Facilities:
 - The following twenty-two Large Facilities participate in our Large Facilities Security Team (Section D.4): Academic Research Fleet (ARF), Cornell High Energy Synchrotron Source (CLASSE/CHESS), Gemini Observatory (Gemini), Geodesy Advancing Geosciences and EarthScope (GAGE), Green Bank Observatory (GRO), IceCube Neutrino Observatory (ICNO), International Ocean Discovery Program (IODP), Large Hadron Collider/ Compact Muon Solenoid (LHC/CMS), Large Synoptic Survey Telescope (LSST), Laser Interferometer Gravitational-wave Observatory (LIGO), Long Baseline Observatory

- (LBO), National Center for Atmospheric Research (NCAR), National Ecological Observatory Network (NEON), National High Magnetic Field Laboratory (NHMFL), National Optical Astronomy Observatory (NOAO), National Radio Astronomy Observatory (NRAO), National Solar Observatory (NSO), National Solar Observatory / Daniel K. Inouye Solar Telescope (NSO/DKIST), National Superconducting Cyclotron Laboratory (NSCL), Natural Hazards Engineering Research Infrastructure (NHERI), Ocean Observatories Initiative (OOI), United States Antarctic Program (USAP)
- The following Large Facilities have also committed to working on the Trusted CI Framework (Section D.1): Gemini Observatory (Gemini), IceCube Neutrino Observatory (ICNO), Large Synoptic Survey Telescope (LSST), National Ecological Observatory Network (NEON), National Solar Observatory (NSO)
 - Additionally, Eric Cross of the National Solar Observatory (NSO) will serve on our Advisory Committee
- Other NSF centers and projects:
 - We have collaborations with the NSF Science Gateways Community Institute and the NSF Cyberinfrastructure Center of Excellence Pilot Project to co-fund .5 FTE of a security analyst with each.
 - We will collaborate with the Engagement and Performance Operations Center (EPOC) in delivering our train-the-trainers program.
 - The following projects have committed to working on the Trusted CI Framework (Section D.1): XSEDE
 - The following projects have committed to working with our year one Annual Challenge on data integrity: Midwest Big Data Hub, Northeast Big Data Hub, South Big Data Hub, West Big Data Hub.
 - We are working with Dr. Husain at Cal Poly Pomona to provide training to the NSF Scholarship for Service program.
 - We are collaborating with the U. South Alabama (NSF award #1636470) on cybersecurity transition to practice.
 - Regional networks:
 - The following regional networks have committed to our train-the-trainers program (Section D.9): 3ROX, Front Range GigaPOP, Great Plains Network, iLight, KINBER, LONI, NEREN, NJEDge, NYSErNet, OSHEAN, The Quilt, WVNET
 - International partners and other non-NSF projects:
 - The following projects have committed to working on the Trusted CI Framework (Section D.1): Australian National University Cyber Institute, Australian National Computation Institute, ESNet, NERSC, WISE Community
 - The following projects have committed to working with our year one Annual Challenge on data integrity: Indiana Geological and Water Survey, Ostrom Data Initiative
 - We are collaborating with the Campus Research Computing Consortium (CaRCC) to understand the needs of campus research computing centers and ensure our Framework is applicable to them.