Center for Trustworthy Scientific Cyberinfrastructure

The NSF Cybersecurity Center of Excellence

Year One Report

NSF Grant ACI-1547272

January 1, 2016 - December 31, 2016

For Public Distribution

CTSC Team

Andrew Adams[1], Jim Basney[3] (co-PI), Randy Butler[3], Robert Cowles[5], Jeannette Dopheide[3], Terry Fleury[3], Randy Heiland[2], Elisa Heymann[4], Craig Jackson[2] (Co-PI), Scott Koranda[5], Jim Marsteller[1] (co-PI), Prof. Barton Miller[4] (co-PI), Susan Sons[2], Amy Starzynski Coddens[2], Von Welch[2] (PI)

[1]Carnegie Mellon University/PSC
[2]Indiana University/CACR
[3]University of Illinois/NCSA
[4]University of Wisconsin-Madison
[5]Independent Consultant

About CTSC

The Center for Trustworthy Scientific Cyberinfrastructure (CTSC) is funded by NSF's Division of Advanced CyberInfrastructure as the NSF Cybersecurity Center of Excellence (CCoE). In this role, it provides the NSF community a coherent understanding of cybersecurity's role in producing trustworthy science and the information and know-how required to achieve and maintain an effective cybersecurity program. CTSC achieves this mission through a combination of one-on-one engagements with NSF projects, training and best practices disseminated to the community through webinars, and the annual, community-building NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure.

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

Citing this Report

Please cite this report as: Von Welch. NSF Cybersecurity Center of Excellence Year One Annual Report. http://hdl.handle.net/2022/21163

This report describes work supported by the National Science Foundation under Grant Number ACI-1547272. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation. For updates to this report and other reports from CTSC, please visit https://trustedci.org/reports/

Executive Summary

The Center for Trustworthy Scientific Cyberinfrastructure (CTSC) was funded as the NSF Cybersecurity Center of Excellence on January 1st, 2016. This report covers CTSC's first year (January 1, 2016-December 31, 2016) as the NSF Cybersecurity Center of Excellence. It describes CTSC accomplishments under its mission "to provide the NSF community with a coherent understanding of cybersecurity, its importance to computational science, and what is needed to achieve and maintain an appropriate cybersecurity program."

Specific accomplishments detailed in this report include:

- Undertaking one-on-one collaborations ("engagements") to address cybersecurity challenges for Gemini Observatory, WildBook/IBEIS, Array of Things, SciGap, HUBzero, OSiRIS, the TransPAC IRNC network, LIGO, and the US Antarctic Program.
- In collaboration with ESnet, convening a working group of leaders from the open science community to develop an Open Science Cyber Risk Profile.
- Initiating a Situational Awareness service for the NSF community to inform them of security vulnerabilities and the specific impact on NSF CI.
- Hosting the NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure, August 16-18 in Arlington, VA, with 100 attendees.
- Launching a monthly webinar series covering NSF cybersecurity which drew over 160 attendees and 80 subsequent viewings of recordings.
- Providing 15 highly-rated training sessions topics to over 130 CI professionals on cybersecurity topics include identity management, log analysis, secure coding, and related topics at the NSF Cybersecurity Summit, XSEDE, Supercomputing, Indiana University, the Internet2 Technical Exchange, and the eResearch Australasia Conference.
- Partnering with the newly launched Science Gateway Community Institute (SGCI) SI2 Institute to fund half of a security analyst focused on science gateway security. Additional partnerships to ensure a coherent CI ecosystem included ESnet, the Bro Center of Expertise, the EU Authentication and Authorisation for Research and Collaboration project, the REN-ISAC, and the recently-funded NSF CICI Regional Cybersecurity Collaboration projects: CORE, SAC-PA, SCEPTRE, and SouthEast SECURE.
- Conducting our first open Engagement Application period, receiving nine applications and accepting six for 2017.

Table of Contents

1. Introduction

With the official announcement of its new funding and title as the NSF Cybersecurity Center of Excellence, the Center for Trustworthy Scientific Cyberinfrastructure (CTSC) started 2016 running. The launch of the CTSC as the NSF Cybersecurity Center of Excellence generated over a dozen press articles, captured in the CTSC blog[1].

In addition to its mission "to provide the NSF community with a coherent understanding of cybersecurity, its importance to computational science, and what is needed to achieve and maintain an appropriate cybersecurity program," CTSC identified three community goals designed to focus the CCoE's efforts:

1. For all Large Facilities to be confident in their information security programs.
2. For all NSF projects to have the information they need to be confident in their information security programs.
3. Fully understanding the role of cybersecurity in producing trustworthy science.

This report covers the the NSF Cybersecurity Center of Excellence's first year (January 1, 2016-December 31, 2016). It is organized by three activity themes - Building Community, Sharing Knowledge, and Collaborative Engagements - and then followed by sections describing the Center's Advisory Committee, Metrics, Accomplishments, Lessons Learned and Adjustments, and concludes with planned points of emphasis for 2017.

2. Building Community

This section covers activities by the NSF Cybersecurity Center of Excellence to build a NSF community sharing experiences, lessons learned, and effective practices around cybersecurity in the context of NSF science.

2.1. Benchmarking Survey

In 3Q2016, we began socializing and collecting responses on a benchmarking survey designed to collect and aggregate information about cybersecurity in the NSF science community. The goal is to provide the the NSF science community, the CCoE, and other stakeholders a baseline view, and facilitate an understanding of changes over time. The survey includes questions on topics including cybersecurity budgets, type and frequency of security incidents, and most-used best practices resources and frameworks, as well as topics suggested by the community in response for our request for input.[2] We will issue a report analyzing the results in early 2017.[3]

[1] http://blog.trustedci.org/2016/01/ctsc-funded-as-nsf-cybersecurity-center.html

[2] http://blog.trustedci.org/2016/06/help-ctsc-build-our-community.html

[3] Our initial timeline called for report publication in 4Q2016. We extended that timeline due, in part, to extending our response period to increase the response rate.

2.2. Large Facility Outreach

NSF Large Facilities (https://www.nsf.gov/bfa/lfo/) continue to be an emphasis for CTSC due to their visibility and to support one of the CCoE's three community goals: *"For all Large Facilities to be confident in their information security programs"*. In the first year of the CCoE, we continued engaging the Large Facilities and broader CI community by hosting the NSF Cybersecurity Summits for Large Facilities and Cyberinfrastructure. These events have been invaluable both in terms of building a community among NSF projects, and making the NSF community aware of CTSC. This year featured plenary sessions from three Large Facilities: LIGO, GEMINI, IceCube/Division of Polar Programs.

Additionally, the CCoE participated in the Large Facility workshop that took place Tuesday May 24 through Thursday May 26th at the Ripley Center in Washington, DC. Co-PI James Marsteller presented "The NSF Cybersecurity Center of Excellence: Large Facilities Cybersecurity Resources" as part of a working lunch on the 25th. The presentation included CTSC developed cybersecurity resources, as well as details on the NSF Cybersecurity Summit and Call for Participation. Marsteller also highlighted the expanded situational awareness service offered by CTSC.

Another initiative launched by CTSC in 2017 was the Large Facilities CISO working group. The goal of this initiative is to improve CTSC's understanding of the Large Facilities perspectives and requirements, and to improve communication and information sharing among the LFs. This idea was discussed with the NSF Large Facilities Security working group ("FacSec") in September, who expressed their support for the formation of such a group. To date, eleven Large Facilities are represented on the working group, which more presentation being recruited. CTSC has created a email list for the working group, sent an introductory email, and plans to have an initial kick-off conference call in January 2017.

2.3. 2016 NSF Cybersecurity Summit

We executed the 2016 NSF Cybersecurity Summit August 16-18 in Arlington, VA to the strongest response from the NSF CI community participation to date. One hundred people attended the summit, an 11% increase over the 2015 summit. Representation from 14 Large Facilities made up one quarter of the attendees. This year, the response to the call for participation was exceptionally strong, resulting in 15 plenary proposals, 8 training proposals, 10 student applications and two table talk topics. Initial feedback from the attendees indicate the program content, logistics and active discussions were very successful.

With the completion of the 2016 Summit we are now in the process of reviewing and analyzing the general summit attendee survey as well as the training evaluation

responses. This data will be included the 2016 summit report along with key observations and findings. A draft version of the report will be shared first with the summit organizers and program committee before a publishing a final version at http://trustedci.org/2016summit/ in early 2017.

Fig 1. Attendees from the 2016 NSF Cybersecurity Summit.

2.4. Webinar Series

We launched the CCoE Webinar Series (https://trustedci.org/webinars/) on May 23rd with an overview of CTSC and how it can serve the community. The talk was presented by members of the leadership team. Six monthly talked followed, from members of the CTSC project team as well as invited talks from the community. The following table shows the number of webinar attendees and archive viewers in 2016:

Table 1. CTSC Webinar attendance and archive viewing.

Date	Topic	Speaker	Attended[4]	Watched Later
May	CCoE Intro	CTSC PIs	18	4
Jun	Risk Self Evaluation	Fleury	13	3
Jul	XSEDE Info Sharing	Marsteller	6	3
Aug	Science DMZ	Sinatra	44	56
Sep	Open Source	Nalley	15	6
Oct	Science or Security	Strawn	26	10
Dec	Regional Coordination	CICI PIs	38	0
Total			**160**	**82**

2.5. Science Gateway Community Institute Partnership

The Science Gateway Community Institute (SGCI) received a major award as one of two NSF Scientific Software Innovation Institutes (S2I2) on August 1. SGCI and CTSC are partnering to co-fund (25% each) a half-time FTE (Randy Heiland) to help address security issues for science gateways.

[4] Does not include CTSC staff and presenters.

At the Gateways 2016 conference (San Diego, Nov 2-3), Heiland gave a presentation that provided an overview of CTSC and described how we contribute to the security of science gateways. He also gave a in-depth tutorial to 21 attendees on Secure Software Engineering.

On November 29, Heiland attended a day-long planning session with the SGCI Incubator team (at Purdue University). The meeting offered an opportunity to get to know each other and plan for a week-long training session in spring 2017. Some of the topics to be covered at this training will be: intellectual property, sustainability, usability, software engineering, and security for science gateways.

Figure 2. CTSC contributing to discussions at the Gateways 2016 conference.

Figure 3. CTSC at the SGCI Incubator kickoff planning meeting.

2.6. AARC Partnership

We continued our collaboration with the European Authentication and Authorization for Research Collaboration (AARC) project[5] on international interfederation, managing virtual organization membership attributes, and establishing achievable levels of assurance for federated identities used by research communities. This collaboration is now being managed as a "partnership" rather than an "engagement," meaning it is a long-lived coordination activity designed to coordinate practices between the NSF community served by CTSC and the EU constituency served by AARC. In 2016 we focused on training. CTSC and AARC staff met in June to review training slides that were used as input for training at the Cybersecurity Summit in August.

2.7. Presentations

CTSC's outreach efforts, both to educate the community on cybersecurity for science and raise awareness of CTSC's services, included presentations at the Terena Networking Conference, the Educause Cybersecurity Professional Conference, the Internet2 Global Summit, and a keynote address at the First International Conference on the Internet, Cyber Security and Information Systems. For a full list of CTSC's presentations, please visit http://trustedci.org/presentations/.

Fig 4. Co-PI Jim Basney presenting CTSC at the Terena Networking Conference
Credit Adam Slagell:
https://twitter.com/slagell/status/742980116586856448

Fig 5. PI Von Welch presenting CTSC at the Southern Partnership in Advanced Networking (SPAN) workshop.

3. Sharing Knowledge

This section covers activities by the NSF Cybersecurity Center of Excellence to create and distribute knowledge regarding cybersecurity in the context of NSF science.

[5] https://aarc-project.eu/

3.1. Open Science Cyber Risk Profile[6]

In collaboration with ESnet, specifically Sean Peisert and Michael Dopheide, CTSC organized a working group of community experts to draft an Open Science Cyber Risk Profile (OSCRP). The goal of the OSCRP is to provide scientist, naive to security, a resource enabling them to frame, scope, and understand risk within open science projects. The OSCRP provides an enumeration of common scientific assets and the associated risks related to cybersecurity for each, allowing scientists to put the risks into the context of their assets and hence their science.

Core members of the OSCRP working group are:

- RuthAnne Bevier, Caltech
- Rich LeDuc, Northwestern
- Pascal Meunier, HUBzero
- Steve Schwab, ISI
- Karen Stocks, UCSD

Contributing members were:

- Ilkay Atlintas, SDSC
- James Cuff, Harvard
- Warren Raquel, NCSA/UIUC
- Reagan Moore, iRods

To ensure a broad and accurate perspective of the concerns from the science community, the group invited members of science projects to present to the group. Presentations were made by Tanya Berger-Wolf, Matt Jones, Fred Luehring, and Alex Withers.

The profile is freely available at http://trustedci.github.io/OSCRP/ and is currently in public comment. It has been disseminated in blog posts by ESnet[7], CTSC[8], and in PI Welch's presentation at the NSF Cybersecurity Summit[9].

By hosting the profile on GitHub, a free-to-use repository typically used for hosting software, we hope to enable and foster a sense of community ownership and

[6] The product was originally going to be entitled Open Science Cyber **Threat** Profile, but the name was changed by the working group as they believe the term "risk" was more appropriate given the focus on information assets rather than the external forces creating the risks.

[7] https://esnetupdates.wordpress.com/2016/10/31/working-group-on-open-science-cybersecurity-risks-releases-first-document-draft-for-public-comment/

[8] http://blog.trustedci.org/2016/10/oscrp-draft.html

[9] https://dx.doi.org/10.6084/m9.figshare.3792063.v1

contributions. This idea for this approach was adopted from NIST (https://github.com/usnistgov) and we have seen initial success with good discussion using GitHub's issue tracker: https://github.com/trustedci/OSCRP/issues.

3.2. Situational Awareness

CTSC provided situational awareness (https://trustedci.org/situational-awareness) of current cybersecurity threats to the cyberinfrastructure (CI) of research and education centers, including those threats which may impact scientific instruments. This service is available to all CI community members by subscribing to CTSC's mailing lists.

CTSC staff members monitored several sources for possible threats to CI, including:

- OpenSSL, OpenSSH, and Globus project and security announcements
- US-CERT advisories
- XSEDE announcements
- RHEL/EPEL advisories
- REN-ISAC daily notifications
- Social media, such as Twitter, Reddit (/r/netsec and /r/security), and LinkedIn
- News sources, such as The Hacker News, ARS Technica, Threatpost, The Register, Naked Security, Slashdot, Krebs, SANS Internet Storm Center, Paul's Security Weekly and Schneier

CTSC staff filtered these sources for software vulnerabilities of interest to CI operators and software developers. For those issues which warranted notification to the CTSC mailing lists, we also provided guidance on how operators and developers can reduce risks and mitigate threats. We coordinated with XSEDE and the NSF supercomputing centers on drafting and distributing alerts to minimize duplication of effort and benefit from community expertise. In 2016 we issued 21 software vulnerability alerts to 53 subscribers.

Comments in our December 2016 survey of subscribers emphasized that the Situational Awareness program helps them prioritize and understand issues:

- *"Having CTSC 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 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."

3.3. Publications

In addition reports delivered in the context of engagements and blog posts, CTSC publications this year were:

- Scott Russell, Craig Jackson, Robert Cowles, *Cybersecurity Budgeting: A Survey of Benchmarking Research and Recommendations to Organizations*, presented at and to be published in the report of the 2016 NSF Cybersecurity Summit, Arlington, VA, 17 Aug 2016. The presentation included a detailed case study of cybersecurity budgeting at Department of Energy labs.
- James A. Kupsch, Elisa Heymann, Barton P. Miller, and Vamshi Basupalli, “Bad and Good News about Using Software Assurance Tools”, Software: Experience and Practice, April 2016. http://onlinelibrary.wiley.com/doi/10.1002/spe.2401/full

3.4. Training

CTSC delivered training to over 150 members of the NSF community in this last year at 7 venues. The NSF Cybersecurity Summit continues to be CTSC’s made venue for delivering training, both directly and by organizing contributions from the community. We’ve organized our training contributions as those related to the Summit and those at other venues.

3.4.1. NSF Cybersecurity Summit Training

Training at the NSF Cybersecurity Summit was driven through an open call for particpation (https://trustedci.org/2016-nsf-cfp/). Through that CFP, CTSC proposed and presented the following training:

- A half day on Developing Cybersecurity Programs for NSF Projects (15 attendees).
- A half-day on secure programming and automated assessment tools (9 attendees).
- A full-day training on Federated Identity Management for Research Organizations (5 attendees). The training covered SAML, Shibboleth, federations (InCommon, eduGAIN), application integration, OpenID Connect, and collaboration management.

- A half-day training on Secure Software Engineering Best Practices (13 attendees). This training was newly developed by CTSC in 2016.

Additionally, members of the NSF community proposed and presented the following training at the Summit:

- The Bro project, in collaboration with CTSC, presented a full-day Log Analysis Training (17 attendees).
- The REN-ISAC presented a 30-minute introduction to cyber threats as an introduction to our Developing Cybersecurity Programs training.
- Anurag Shankar of Indiana University presented a half-day training session on Building a NIST Risk Management Framework for HIPAA and FISMA Compliance (9 attendees).
- Phil Salkie of Jenariah Industrial Automation presented a half-day training on Securing Legacy Industrial Control Systems (14 attendees).
- Steve Tuecke of the University of Chicago presented a half-day training on Building the Modern Research Data Portal Using the Globus Platform (7 attendees).

Complete descriptions of the training sessions at the Summit may be found at https://trustedci.org/2016training/.

3.4.2. Other training Delivered

In addition to the NSF Cybersecurity Summit, CTSC proposed and was accepted to provide training at other major venues:

- We developed and presented a short one-hour version of our cybersecurity program training targeted to small to medium sized NSF projects. The initial presentation of this training was at Indiana University on April 27th and was attended by 6 members of the NSF community and local information security office.
- We presented our training on "Federated Identity Management for Virtual Organizations" at the Internet2 2016 Technology Exchange (15 attendees), and the eResearch Australasia Conference in Melbourne, Australia (8 attendees).
- We presented our training on “Secure Coding Practices and Automated Assessment Tools” at SC16 (20 attendees). This is first time we’ve observed reviewer enthusiasm for security topics at Supercomputing: “This tutorial is timely (and probably timeless) as security issues persist in software. These issues

are applicable to all software including that in the HPC arena. I believe the SC audience is less likely to be aware of security issues in code, or at least the specifics, and will benefit quite a bit from attending this tutorial."

- We presented a half-day long tutorial on "Secure Programming and Automated Assessment Tools" at XSEDE16. There was a modest (10 attendees) but very engaged group, and they asked many relevant questions throughout the tutorial and continued well past the end of the sessions. The attendees understand the importance of the content of the tutorial for the XSEDE community, and believe that a tutorial like this should be mandatory for any member of the XSEDE community.
- We presented our training on "Secure Software Engineering Best Practices" at Gateways 2016 (21 attendees) as part of our partnership with the Science Gateway Community Institute.

3.4.3. Software Security Course Development

We continue to make progress in the development of an university course on software security. In addition to expanding the modules we use in our tutorials, we created new modules on security for mobile apps in Android, including issues more specific to the mobile world, such as bad programming practices for error handling dealing with WebView, insecure data storage, and weak server-side controls. We also developed a module to teach security by design using threat modeling. This module complements the different visions needed when addressing software security: thinking like a manager, like a designer, and like an analyst.

We will start recording the video lectures for the above modules start January 2017. In addition, we will start the development of the practical exercises for the course. There will be five exercises: security at the design step with threat modeling, a vulnerability assessment exercise using First Principles Vulnerability Assessment (FPVA), practical experience with automated assessment tools for C/C++ and Java, using several tools through the SWAMP, and a practical exercise on Fuzz testing.

3.5. Broader Impacts of CTSC

The CTSC-developed training materials are having a broader impact outside the project including:

- We taught a week-long course at the Universidad Nacional de Asunción, in Paraguay. The attendees were Masters degree students and students in their last year of their computer science degree. The number of attendees was 32. In addition to the lectures and in-class exercises, the students had two weeks after

the course to perform a project using automated assessment tools and the SWAMP (https://continuousassurance.org/). The results were extremely positive. One of the students works for their national center of cyber-security, and the material we taught was new for her, and now she intends to bring the material we taught and the SWAMP back to her agency. In addition, the feedback from the students as for issues they found in the SWAMP was given to the SWAMP User Experience team to help improving the SWAMP.

Fig 6. Prof. Barton Miller and Dr. Elisa Heymann teaching CTSC-developed training in Paraguay and at the NATO-organized Maritime Cyber Security Conference.

- We attended a NATO-organized Maritime Cyber Security Conference at the NMIOTC (NATO Maritime Interdiction Operational Training Centre) on Crete, Greece. Our talk was about applying our First Principles Vulnerability Assessment to the critical software that manages container shipping.

- ScienceNode published two articles during this quarter regarding cybersecurity for science[10,11] -- both a result of the publicity around the launch of CTSC as the Cybersecurity Center of Excellence and our subsequent discussions with the ScienceNode editorial staff.

- Previous projects with whom we have engaged often mention CTSC in their presentations. For example,

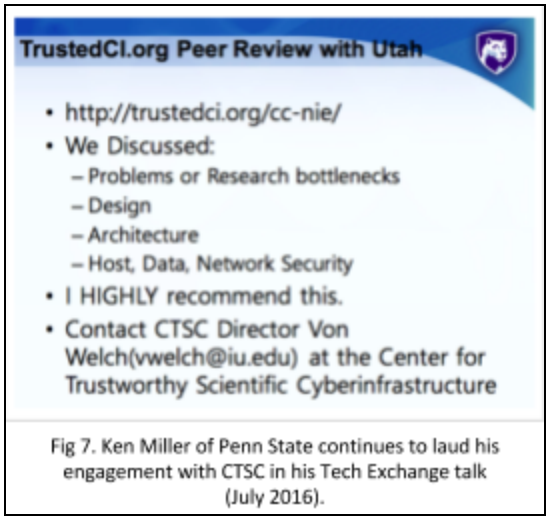

Fig 7. Ken Miller of Penn State continues to laud his engagement with CTSC in his Tech Exchange talk (July 2016).

[10] https://sciencenode.org/feature/what-does-security-mean-in-science-today.php
[11] https://sciencenode.org/feature/securing-the-scientific-workflow.php

the slide from Ken Miller of Penn State in Fig 7.

- CTSC participated in the National Strategic Computing Initiative (NSCI) High-Performance Computing Security Workshop September 29th and 30th at National Institute of Standards and Technology in Gaithersburg, Maryland[12]. The two day workshop was established by Executive Order 13702 to create a National Strategic Computing Initiative. Stakeholders from academia, Government and Industry conferred to identify common security principles, priorities and to identify gaps to address. The workshop was a first step in coordinating security practices across national HPC communities.

4. One-on-One Collaborations (Engagements)

This section covers engagements by the NSF Cybersecurity Center of Excellence, that is collaborations with specific NSF projects and facilities to tackle their specific challenges with cybersecurity in the context of NSF science.

4.1. Engagement Application Process

In 2Q2016, due to demand for engagements surpassing our ability to undertake them, we deployed a new engagement application process (https://trustedci.org/application). In 3Q2016, we actively publicized the application process to the NSF community at large and received 9 applications. In 4Q2016, we notified applicants of our decisions.
In our first cycle, we received 9 engagement applications. We declined 3 applications with feedback for future submissions, deferred 1 application, and accepted the following 5 applications for engagement in 1H2017:

- TransPAC (NSF IRNC Award 1450904)
- OSiRIS (CC*DNI DIBBS Award 1541335)
- DataONE (ACI, CSE #1430508; previously ACI #0830944)
- University of New Hampshire Research Computing Center
- HTCondor-CE (PHY-1148698)

4.2. Engagement Evaluations

We successfully piloted our Engagement Evaluation Questionnaire with Gemini Observatory. By formalizing and bringing some quantifiable results to the engagement follow-up process, we hope to facilitate impact measurement over time (e.g., impacts of an engagement immediately following the engagement, six months following, one year following), as well as aggregate and cross-engagement analysis on common criteria. We will plan to use this tool across all our engagements.

In addition to Gemini, we received initial evaluations from Science Gateway Platform as

[12] https://www.nist.gov/news-events/events/2016/09/nsci-high-performance-computing-security-workshop

a Service (SciGaP), Array of Things (AoT), Wildbook/Image-Based Ecological Information System (IBEIS), and the United States Antarctic Program engagees. We received an average rating of 4.8 to the question, "On a scale of 0 - 5, rate the positive impact of the engagement on the project or facility," where 0 is "no positive impact" and 5 is "strong positive impact." No respondent reported negative impact. All respondents gave a 5 rating ("Extremely Likely") to the question, "How likely are you to recommend that other researchers, projects, or facilities engage with CTSC?"

As we gather more evaluations in 2017, we will report on additional trends that emerge, including indicators of ways we can improve our engagement processes and impacts.

4.3. Array of Things

CTSC completed an engagement with the Array of Things (AoT, NSF ACI award #1532133). The AoT project is, in collaboration with the City of Chicago, developing and deploying a network of interactive, modular sensor boxes that will be installed around Chicago. These sensors collect real-time data on the city's environment, infrastructure, and activity and make that data available for research and public use.

Fig 8. Array of Things privacy policy public meeting in Chicago.
https://twitter.com/SustainTheChi/status/742877930817228801

CTSC completed an assessment of AoT's cybersecurity, advised AoT and the City of Chicago's CIO on best practices for developing privacy policy, and assisted them in processing the feedback they received on their draft privacy policy from privacy advocates and Chicago residents to produce their initial Operating and Privacy policies[13].

4.4. Gemini Observatory

We completed an engagement started by the previous CTSC project (NSF award 1234408) with the Gemini Observatory.

In the late Fall and early Winter of 2015/2016, CTSC and Gemini executed an engagement plan focused on core policy processes and documentation, as well as a close unified look at ICS/SCADA, technical, and physical controls at Gemini North.

The engagement's policy work focused on initiating a draft Policy Development Protocol, and updating Gemini's core policy documentation (e.g., beginning a Master

[13] https://arrayofthings.github.io/final-policies.html

Information Security Policy and revising Gemini's AUP). CTSC gave feedback on existing documentation, advice on the policy development lifecycle, and guidance on how best to utilize CTSC's policy templates[14]. Gemini developed a priority list and timeline for the development/revision and implementation of these and additional policies.

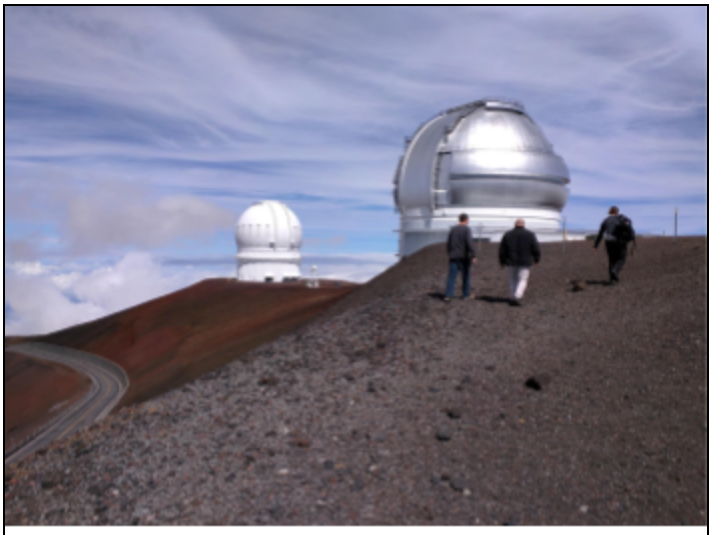

Fig 9. CTSC's Susan Sons and Gemini personnel on Maunakea.

CTSC staff performed a site visit to the Gemini North facility to inform detailed recommendations for improving the physical security and technical security of instrument and industrial control / SCADA systems critical for Gemini's scientific mission. The visit included inspection tours of the base facility in Hilo, the mid-point facility at Hale Pohaku, and the actual telescope atop Maunakea at 14,000 feet. CTSC interviewed eight Gemini staff members concerning IT support, physical security, ICS/SCADA systems, MS Windows security, web application development, and operational application support. CTSC conducted a physical penetration test of the Base facility, which was thwarted an attentive Gemini staffer. The depth and breadth of this fact-finding mission enabled CTSC to produce a report providing detailed recommendations for enhancements to both physical security and cybersecurity from an on-the-ground point of view.

Gemini gave the engagement high ratings in the Engagement Evaluation Questionnaire, and identified the following areas where the engagement helped improve cybersecurity:

- Improved governance / policy / risk acceptance structure,
- Knowledge / documentation of information assets,
- Understanding cybersecurity risks to the science mission,
- Communication of risks to decision-makers and stakeholders,
- Increased cybersecurity knowledge among staff and personnel,
- Effective use of resources in promoting best practices,
- Selection of better technology or services,
- Improved security of software we are developing

In terms of broader impacts, Gemini stated, "Our managing organization, AURA, and

[14] See, http://trustedci.org/guide

subsequently our sister observatory, NOAO, have received some of the recommendations and insight that were produced through this engagement and are evaluating possibilities of implementation."

Chris Morrison, stated:

> *"I have said this on multiple occasions, but I am being absolutely sincere when I say that the engagement was an outstandingly professional, humbling, enlightening and enjoyable experience. We are incredibly pleased to have been able to tap into the knowledge and expertise of the amazingly talented group of people that make CTSC what it is. I will recommend the CTSC engagement to anybody without a second thought and look forward to further consultations and follow up engagements if at all possible. Thank you kindly for pointing us in the right direction and providing us with the tools that we needed to refocus our efforts. Chris M."*

4.5. HUBzero

CTSC engaged with the HUBzero project[15] to help their cybersecurity program mature in the face of an internal re-organization, growing/maturing software development efforts, and research and development foci. HUBzero's reorganization made it more important to have clear roles and responsibilities around security, clear communication paths, and preparation for vulnerabilities and incidents. CTSC helped HUBzero to write and adopt a Master Information Security Policy and Procedures document to lay out the project's overall strategy, roles, and responsibilities as well as point staff members to the other security documentation they should be aware of.

HUBzero's development team has been maturing in terms of engineering rigor, but has not formalized its process to the point that it is easy to ensure internal consistency, iterate on process, and communicate to internal stakeholders. CTSC aided HUBzero in formalizing security-critical software engineering practices into a Software Assurance and Testing Policy document that the project can iterate on over time. CTSC also worked with HUBzero's new Research and Development team to aid them in getting security addressed as early in the R&D process as possible, and communicate the needs of R&D products to those who will ultimately maintain them.

As of the end of 2016, we have nearly completed the engagement with HUBzero and will do so in early 2017.

4.6. LIGO CISO Search

Continuing its practice of innovation with engagements, CTSC undertook a engagement with the Laser Interferometer Gravitational-Wave Observatory (LIGO) project,

[15] http://blog.trustedci.org/2016/10/ctsc-set-to-work-with-hubzero.html

specifically Stuart Anderson at CalTech, to assist in their search for a new Chief Security Officer. CTSC helped LIGO distribute the job posting to the NSF and higher education cybersecurity communities.

The position was successfully filled by LIGO/CalTech. While it is not apparent that CTSC's efforts helped, it was a relatively low effort activity by CTSC (and will be easier in the future now that we have undergone the process once) and we plan to offer similar assistance in the future.

4.7. Multi-Institutional Open Storage Research Infrastructure

In October 2016 we launched an engagement with the Multi-Institutional Open Storage Research Infrastructure project (MI-OSiRIS, NSF ACI award #1541335), which is evaluating a software-defined storage infrastructure for the primary Michigan research universities. The CTSC-OSiRIS engagement focuses on federated identity and access management with InCommon, Shibboleth, and COmanage, addressing the novel challenge of integrating federation technologies with the Ceph distributed object store technology. The engagement is conducting a review of the OSiRIS Access Assertion design, including 1) a review of use cases, 2) documentation of existing mechanisms considered, leveraged, and extended (e.g., SAML, X.509, JWT), 3) documentation of assets, interfaces, threats, and security controls, and 4) code review. As of December 2016, the engagement team has reviewed use cases and begun reviewing threats and controls.

4.8. SciGaP

We completed an engagement started by the previous CTSC project (NSF award 1234408) with the Science Gateway Platform as a Service (SciGaP, NSF ACI award #1339774) project (https://scigap.org/). Our final reports for this engagement are public and available at https://trustedci.org/scigap/.

CTSC and SciGaP collaborated to design the security and identity management functionality of services that support science gateways. The engagement covered a very broad range of security topics that affect science gateways, e.g., trust models; authentication and authorization; identity and access management; and software assurance. The SciGaP PI, Marlon Pierce, concluded that it was a "*highly productive engagement that led directly to SciGaP's current security infrastructure implementation*". In response to a CTSC follow-up survey question: "How has this engagement improved cybersecurity for your project or facility?", Pierce replied:

> *"Increased cybersecurity knowledge among staff and personnel. Selection of better technology or services. Improved insight into software we are developing.*

Improved security of software we are developing. More secure or efficient identity and access management practices."

4.9. TransPAC

The IRNC TransPAC4 project (NSF ACI award #1450904) is independantly developing a cybersecurity program using our Guide (https://trustedci.org/guide/). We continue to offer them occasional support by answering questions.

4.10. United States Antarctic Program

In December, CTSC and the National Science Foundation's Office of Polar Programs wrapped up an engagement focused on the United States Antarctic Program[16] (USAP) processes and policies relevant to polar science information security. CTSC produced a report focused on the present state of infosec integration and opportunities for improvements, entitled "Integrating Information Security into USAP's Science Project Lifecycle".[17] During the course of the engagement, CTSC reviewed over 110 artifacts and interviewed four representatives of polar science projects and facilities. Additionally, CTSC and USAP held 12 calls with NSF and Leidos staff.

This engagement presented a unique opportunity for CTSC to engage directly with the people and program that facilitates all US science in Antarctica. The CTSC team approached this engagement from the viewpoint of PIs, researchers, and grantee personnel, mapping their experience integrating with USAP's processes and infrastructure. The report included a factual summary of information security information provided in various phases from proposal to deployment to the ice; opportunities for improvement; and potential areas for future collaborations. The opportunities ranged from event timing, clarification and usability, and improved information security for the science projects. CTSC provided appendices listing the artifacts reviewed, a detailed event timeline from the grantee point of view, and detailed comments on selected artifacts.

Antarctica is an incredibly important and challenging environment for science and the use of technology. Its remoteness and harsh environment stretches the boundaries of where the Internet and other utilities we take for granted can reach and function. The logistics of moving people and technology from hundreds of different institutions on and off the ice is challenging, indeed. CTSC engagement team was honored to have the opportunity to learn about the polar science process and talk to some of the people who make it happen. We hope the report is a valuable input.

[16] https://www.usap.gov/

[17] For more information regarding the engagement deliverables, please contact Tim Howard, USAP Information Security Manager, tghoward@nsf.gov.

In its immediate post-engagement evaluation, USAP selected the following areas where the engagement helped improve cybersecurity: “Communication of risks to decision-makers and stakeholders”; “Increased cybersecurity knowledge among staff and personnel.”

NSF manages the USAP to enable NSF-funded polar research carried out by grantees at colleges and universities nationwide. Within NSF Office of Polar Programs, the Antarctic Infrastructure and Logistics Section (AIL) manages the support systems for the field science, primarily through the Antarctic Support Contractor, Leidos. These functions include station operations, logistics, information technology, construction, and maintenance. USAP has a goal of maximizing grantees’ effective integration of information security planning and implementation into that lifecycle.

4.11. Wildbook/IBEIS

Fig 10. CTSC-Wildbook presentation at July 2016 International Conference on Computational Sustainability (http://www.compsust.net/compsust-2016/)

In the first half of 2016, CTSC and the Wildbook (ibeis.org, NSF EF award #1550881, formerly called IBEIS) project collaborated on the development of a role-based access control (RBAC) prototype for the next generation Wildbook platform. The goal of the collaboration was to establish an RBAC design to support the variety of image gathering, curation, and analysis workflows across multiple ecological communities (studying Grevy's Zebras, Sea Turtles, Geometric Tortoises, Whale Sharks, Humpback Whales, Dolphins, etc.) while maintaining animal privacy (e.g., protection from poaching/trafficking).

Fig 11. Wildbook/IBEIS comments on Twitter in regard to their engagement with CTSC. https://twitter.com/IBEIS_org/status/751155960190828545

CTSC and Wildbook implemented an RBAC prototype using the open source wso2.com software, which implements the System for Cross-domain Identity Management (SCIM) and eXtensible Access Control Markup Language (XACML) standards. This prototype defined multiple roles and access policies as shown in Table 2

Table 2. Roles and access policies defined in CTSC-IBEIS engagement.

Roles	Policies
Media Asset Contributors Annotation Contributors Data Curators Data Managers Organization Members (Users) Organization Administrators Platform Administrators	Create/Read/Update/Delete media assets, annotations, encounters, etc. Assign roles to users Share org A data with org B Access to APIs

The prototype demonstrated the ability to implement access policies using the XACML Subject-Resource-Action pattern. Table 3 shows some examples.

Table 3. Example access policies implemented in CTSC-IBEIS engagement.

Subject (Role)	Resource	Action
Organization Member	Media Asset	Create/Read
Data Curator	Annotations	Create/Read/Update/Delete
Organization Administrator	Organization Policy	Create/Read/Update/Delete
Platform Administrator	Organization	Create/Read/Update/Delete

Tanya Berger-Wolf (Wildbook) and Jim Basney (CTSC) presented the results of the collaboration at the July 2016 International Conference on Computational Sustainability (http://www.compsust.net/compsust-2016/). Dr. Tanya Berger-Wolf included CTSC staff in her presentation at the White House Frontiers conference presentation[18] on IBEIS/WildBook.

5. Advisory Committee Meeting

We held our half-day CTSC Advisory Committee meeting in Salt Lake City on November 14th during Supercomputing 2016. All four current members of our Advisory Committee attended: Tom Barton (U. Chicago), Neil Chue Hong (UK Software Sustainability Institute), Nick Multari (PNNL), and Nancy Wilkens Diehr (SDSC and Software Gateway Sustainability Institute). Additionally Kevin Thompson (NSF) attended as an observer. A

[18] http://frontiersconference.org/tracks/national (12:10-18:00 in the video)

set of recommendations is currently in draft form and has been shared with the committee and NSF.

Our Advisory Committee lost two members this year: Don Middleton retired from NCAR and Greg Bell left ESnet. We received advice from the four current members on replacements and expect invite two additional members in time for next year's meeting.

6. CTSC Cybersecurity Program

Since the inception of the initial cybersecurity program, CTSC has produced a framework for developing cybersecurity programs tailored to the NSF cyberinfrastructure (CI) community titled the "Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects" also known informally as the Cybersecurity Planning Guide or CPG. With the launch of the CCoE, CTSC rewrote its cybersecurity program to align with this guide. The objectives of this cybersecurity program revision were: 1) Update CTSC's Cybersecurity core cybersecurity policies and procedures documents in line with the CPG templates, risk assessment tools and overall methodology; 2) Verify that the policies and procedures to protect CTSC assets within the documents are implemented/enforced, where possible; and 3) Audit all CTSC information resources to verify proper access control. The new cybersecurity program is available on our website: http://trustedci.org/cybersecurity-program/.

7. Metrics From Our Proposal Project Plan

Table 4. CTSC activity goals and achieved metrics.

Activity	Measurement Technique	Goals	Achieved
Engagements with NSF projects.	Direct measurement of the number of engagements.	4-6/year depending on complexity.	On track. Four completed (IBEIS, Gemini, LIGO, and AoT). Three new engagements started (HUBzero, USAP, OSIRIS) with two nearing completion.
	Post-engagement survey.	High ratings of engagement utility.	We successfully piloted our Engagement Evaluation Questionnaire with four engagements. See Section 4.2 for results.
NSF projects using our best practices, guides, threat model to develop and maintain their own cybersecurity programs.	Reported by NSF projects.	Initially 2-4/year using cybersecurity program guide. Aim to increase linearly.	To date DKIST, Gemini Observatory, HUBzero, LSST, NCAR, Pittsburgh Supercomputing Center, and TransPAC have used our Guide. We believe there is more usage and are working on a better mechanism to collect this information.
Training	Direct measurement of attendance.	50 members of NSF community per year attending.	151 attendees: Summit 71, SC16 20, IU 6, Gateways 21, XSEDE 10, Tech-Ex 15, eResearch Australasia 8.
	Survey of attendees.	90%+ rating training as valuable.	We surveyed Summit attendees and 97.96% of respondents indicated CTSC-led training was valuable.
Situational Awareness	Direct measurement of number of individuals and NSF projects receiving announcements.	90%+ of Large Facilities receiving announcements by end of YR1. Aim to increase linearly.	Currently 7 out of 24 Large Facilities represented on our list (29%).
	Survey of community receiving information.	75%+ of recipients rating announcements as valuable and providing information they would not otherwise be aware.	In our December 2016 survey, 85% of respondents rated the announcements as valuable and providing information they would not otherwise be aware.

Table 4. CTSC activity goals and achieved metrics (continued)

Activity	Measurement Technique	Goals	Achieved
Summit	Direct measurement of attendance.	90%+ participation of Large Facilities. Strong, diverse participation across the full range of NSF CI projects, and program officers.	One hundred individuals attended, 12 being NSF staff. Forty-four NSF projects were represented, including 22 Large Facilities.
	CFP response rate.	Increasing CFP response rate each year.	CFP submissions: 15 plenary, 8 training proposals, 10 student applications, 2 table talk topics. A notable increase over 2015's 17 submissions and 2014's 12 submissions.
	Surveys of attendees.	Very strong evaluations on attendee surveys.	97.62% overall experience with the summit was good-excellent. 100% reported information discussed at the summit was useful to their work. 97.62% reported that the summit experience overall was above average.
Software Assurance	Post-engagement assurance tool usage by projects, on 3, 6 and 12 month time scale	Linear progression each year on tool use.	Nothing to report yet.
	Number of projects that engage us for the Moderate and Deep Dive levels.	3-4 requests for engagements each year.	Five applicants requested help with software assurance (Moderate) and three requested a code review (Deep Dive).
	Number of groups using online training materials	Linear progression each year.	Nothing to report yet.

8. Accomplishments Relative to our Project Plan

The following table contains the tasks from the supplemental project plan that was part of our proposal to NSF. The rightmost column gives the actual status of activities relative to that project plan.

Table 5. CTSC accomplishments relative to project plan.

Activity Area	Specific Activity	Actual Status
Engagements	AARC	Completed and evolved into long-term partnership.
	Gemini	Completed.
	United States Antarctic Program	Started and on track.
	HUBzero	Started and on track.
	Others not in original Project Plan	Array of Things, LIGO, OSiRIS.
Outreach	Attend Large Facilities Workshop.	Complete.
	Execute live online chats.	Renamed to Webinars and operational. Deven held.
	Conduct annual community survey.	Survey completed and results being analyzed.
	Develop 3 new training sessions.	Completed: Software Engineering Best Pracitces, Log Analysis (in collaboration with the Bro Project), and Cybersecurity Program Development for Small-to-Medium NSF Projects.
Training	Deliver at least 3 training sessions at 2016 Summit	Completed. Five training sessions presented as Summit, one at XSEDE16, and one at IU.
Situational Awareness	Plan and implement processes for monitoring and reporting on vulnerabilities. Enter operations.	Completed. 21 alerts sent in 2016. There are now 53 subscribers to situational awareness alerts, including 18 new subscribers in 2016.
Threat Model	Convene expert NSF/DOE working group. Conduct thorough literature review.	Complete.
	Present early draft at Summit working session. Publish v1 of Threat Model by end of year.	Complete: http://trustedci.github.io/OSCTR/
Summit	Convene program committee and begin planning 2016 Summit.	Complete.
	Execute Summit in August 2016	Complete. One hundred attendees. In process.
	Publish Report in November 2016	Behind schedule. Will release for comment to attendees in early 2017.

Table 5. CTSC accomplishments relative to project plan (continued).

Activity Area	Specific Activity	Actual Status
Software Assurance	Identify a software assurance engagement for late 2016.	We selected and began discussions with OSG to review HTCondor-CR in 2017.
	Deliver training session at 2016 summit.	Completed.
	Execute one related engagement.	Slated for 1-2Q2017.
	Develop MOOC.	Developing online training modules as described in Section 3. Presentation materials complete and recording starts January 2017.
Center Management	CTSC All Hands Meeting in May.	Completed on June 7-8.
	Cybersecurity Plan Review	New Cybersecurity Plan published August 12th.
	Advisory Meeting in November.	Completed on November 14th.
	Conduct first PDSA cycle.	Completed in line with our face-to-face All Hands meeting in June, our major Study activity for the first half of the year.
	Conduct second PDSA cycle.	Completed in line with our Advisory Committee Meeting, our major Study activity for the second half of the year.

9. Lessons Learned and Adjustments

9.1. Personnel Changes

Randy Butler and Adam Slagell have withdrawn from CTSC and co-PI Jim Basney is now leading the NCSA's CTSC team. This resulted in a re-budget at NCSA transferring effort from Senior Personnel to Other Personnel, enabling NCSA to hire an additional full-time Research Programmer to assist with project engagements and other center activities. With Randy Butler stepping down as co-PI, Bart Miller has stepped up and taken on the role of a project co-PI.

9.2 Advisory Committee Changes

Don Middleton has retired from NCAR and stepped down from the CTSC Advisory Committee. Greg Bell has departed ESnet and also stepped down from the CTSC Advisory Committee. We solicited input from the remaining four advisory committee members in November and plan to invite placements to that committee in 2017.

9.3. Preceding MOOC with On-line Training

We have started developing the suite of online training modules in secure programming and software assurance tools that will be the foundation of our software assurance massive open online course (MOOC). We will complete these modules and use them as the foundation of the lecture portion of the MOOC. As a result, we concentrate on these online modules and related materials in 2016 and the first half of 2017, and then will shift completing development of the MOOC later in 2017. The presentation materials (slides) are 95% done, so recording and editing online modules is the current activity.

9.4. Long-term Partnerships

We have recognized the value in CTSC establishing longer-term collaborations with projects such as ESNet, the Science Gateway Community Institute, and European AARC project in order to foster coherent cybersecurity between the NSF community and the broader open science community. CTSC's partnerships are recognized at http://trustedci.org/partners/.

9.5 CTSC / NSF Cybersecurity Center of Excellence Branding

We recognized a branding issue with our project having two titles: the "Center for Trustworthy Scientific Cyberinfrastructure (CTSC)" and the "NSF Cybersecurity Center of Excellence." After consulting with our advisory committee, NSF, and the Cyverse project (who recently changed their name from "iPlant") we plan on shifting our emphasis from CTSC to the NSF Cybersecurity Center of Excellence. The goal is to emphasize the "NSF Cybersecurity Center of Excellence" title while maintaining any brand recognition in "CTSC" and avoiding confusion. We will take this change on starting in 2017 and have engaged Indiana University's IT communications office for assistance.

9.6 Community Demand for Software Assurance

Demand for engagements (particularly software assurance related engagements) is outpacing our ability provide the services. Of the 9 engagement applications we've received in our open call for Engagements (see Section 4.1), 5 expressed interested in software assurance-related technology evaluation and 3 expressed interest in code review. We were not able to accept all engagements currently under review, at least not for early 2017 execution. While we see this as "a good problem to have," we are also considering whether and how we might scale to meet the demand.

10. Planned Emphasis for 2017

In project year 2, corresponding to calendar year 2017, we will continue our core activities: the NSF Cybersecurity Summit, Training, Situational Awareness, Webinars, Engagements, Community Survey, Outreach and Dissemination of Best Practices. New

areas of emphasis will be:

- **Small-to-Medium NSF Projects**: While the number of NSF projects that CTSC interacts with is impressive, we recognize it is a fraction of the entire NSF ecosystem, particularly for small-to-medium projects. While some of our activities(e.g. blog posts, email lists, webinars, best practices publications) are scalable, and some of our engagements have broad impact (e.g., our engagement with USAP impacts the polar science community), we recognize the challenge in scaling to the entire NSF community We will undertake a strategy of working with projects such as ACI-REF (https://aci-ref.org/), the SI2 software institutes, universities and other organizations that house and serve NSF projects to work through them to foster a understanding cybersecurity, privacy, and identity management issues among the NSF community more broadly.

- **Software Assurance**: While our engagement requests show growing interest from the community around software security, there is no documented, community produced set of expectations for software developers regarding security there does not exist a consistently agreed to and documented set of expectations for software developers regarding security. We have recently convened a Chief Information Security Officer (CISO) working group from the NSF Large Facilities (see Section 2.2) and plan to work with that group to define a set of basic expectations which can then be fed back to the community.

- **Open Science Cyber Risk Profile maintenance**: Having delivered an initial draft of the profile, we will monitor and respond to community feedback and seek to determine and implement practices to make this a sustained community document. We will update the document on an annual basis, using a working session at each year's summit for community input. Significant changes will be circulated to the community for feedback before publication.

- **Increased Outreach to Large Facilities**: We will increase our outreach to Large Facilities to achieve our goal of participation by 90%+ of Large Facilities in CTSC activities.

- **Increased Emphasis on Dissemination of Our Work**: We will publish a journal paper about CTSC (to, e.g., IEEE Security and Privacy). Produce additional technical reports to enable transition to practice and broader impact. Track citations to measure impact.

11. Conclusion

CTSC has a successful first year as the NSF Cybersecurity Center of Excellence with a set of strong accomplishments towards its vision "to provide the NSF community with a coherent understanding of cybersecurity, its importance to computational science, and

what is needed to achieve and maintain an appropriate cybersecurity program." Highlights include engagements with eight NSF projects, drawing one hundred members of the community to the NSF Cybersecurity Summit, initiating situational awareness and cybersecurity webinar series, publishing the Open Science Cyber Risk Profile, and training over 130 NSF CI professionals. CTSC's plans for 2017 include increasing its engagement with the NSF large facilities, while broadening its impact on small-to-medium NSF projects, and taking on the challenge of software security.