Center for Trustworthy Scientific Cyberinfrastructure

Final Report

NSF ACI Grant # 1234408

Covering Project Year 4 (No Cost Extension)

October 1, 2015 - September 30, 2016

CTSC Team

Andrew Adams[1], Jim Basney[3] (co-PI), Randy Butler[3] (co-PI), Robert Cowles[6], Jeannette Dopheide[3], Terry Fleury[3], Randy Heiland[2], Elisa Heymann[4], Craig Jackson[2], Scott Koranda[5] (co-PI), Jim Marsteller[1] (co-PI), Prof. Barton Miller[4] (Senior Personnel), 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
[5]University of Wisconsin-Milwaukee
[6]Independent Consultant

This report describes work supported by the National Science Foundation under Grant Number OCI-1234408. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

For updates to this report and prior reports from CTSC, please see http://trustedci.org/reports/

Executive Summary

The Center for Trustworthy Scientific Cyberinfrastructure (CTSC) transformed and improved the practice of cybersecurity and hence the trustworthiness of NSF scientific cyberinfrastructure (CI) and the science it produces. CTSC provided the NSF CI community with cybersecurity leadership, expertise, training, and the nexus of a community for sharing experiences and lessons learned. The vision of CTSC is an NSF CI community in which each project knows where it fits in a coherent cybersecurity ecosystem, has access to the tools and expertise to enact a cybersecurity program that efficiently support science, participates in the sharing of experiences and collaboration between projects and is greatly benefited by leveraging services from universities, regional and national networks (e.g., CIC, SURA, Internet2).

This report covers CTSC project year four, a no-cost extension from October 2015 through September 2016. Funding largely expired by the end of 2015, meaning the reported activities and accomplishments were minimal compared to prior project years. During this time, the CTSC PIs involved received notification from NSF that their proposal for an NSF Cybersecurity Center of Excellence was funded to start in January of 2016. This led to some transition activities to ensure the newly funded Center of Excellence could carry CTSC's work forward.

Overall, CTSC was a great success and laid the groundwork for the Cybersecurity Center of Excellence. Through its four years, CTSC engaged with 22 NSF projects (9 new in year three), and trained nearly 300 CI professionals representing over 60 NSF projects. Those numbers include a significant impact on NSF Large Facilities, who comprised 7 CTSC engagees, 15 of the projects who have attended a Summit and benefitting from CTSC's training.

This report describes CTSC's year four activities in details, concluding with a set of lessons learned by CTSC over its four years.

Table of Contents

Introduction: CTSC Overview and Vision

The Center for Trustworthy Scientific Cyberinfrastructure (CTSC) is transformed and improved the practice of cybersecurity and hence trustworthiness of NSF scientific cyberinfrastructure (CI) and the science it enables. CTSC is provided readily available cybersecurity expertise and services, as well as leadership and coordination across a range of NSF scientific CI projects via a series of engagements, best practices, online and in-person training. CTSC re-started the annual NSF Cybersecurity Summits for Large Facilities and Cyberinfrastructure, and hosted three Summits, build a critical community sharing experiences in cybersecurity for cyberinfrastructure.

As NSF pushes towards its vision of "a comprehensive, integrated, sustainable, and secure CI" as described in the Framework for 21st Century Science and Engineering[1], cybersecurity plays a key role. Yet the NSF CI community faces strong challenges in implementing cybersecurity. Projects are forced to divert their resources to develop appropriate expertise, address risks haphazardly, unknowingly reinvent basic cybersecurity solutions, and struggle with interoperability [S3I2]. Contributing to the challenge is the fact cybersecurity cannot solved by a single solution. Every project has its own culture, risk tolerance, unique combination of cutting edge and legacy technologies, collaboration patterns, and timelines, making a "silver bullet" unfeasible. Even when security expertise is available within a project, the complex NSF CI ecosystem brings significant challenges in cross-project collaborations and knowledge dissemination. Lessons learned are shared haphazardly between projects. Important institutional knowledge is often lost when a project is completed or key personnel leave the community. Additionally, requiring each CI project to tackle cybersecurity independently is inefficient and often redundant, leading to multiple implementations that do not interoperate and confound the goal of scientific collaboration, data stewardship, and dissemination.

The vision of CTSC is an NSF CI community in which each project knows where it fits in a coherent cybersecurity ecosystem, has access to the tools and expertise to enact a cybersecurity program that supports science, participates in the sharing of experiences and collaboration between projects and is greatly benefited by leveraging services from universities, regional and national networks (e.g., CIC, SURA, Internet2).

Toward this vision, CTSC undertook activities organized into three thrusts: 1) **Engagements** with specific communities to address their individual challenges and deepen CTSC's knowledge of community requirements; 2) **Education, Outreach and Training**, providing the NSF scientific CI community with training, student education, best practice guides, and lessons learned documents; and 3) **Cybersecurity Leadership**, building towards a collaborative, coherent, interoperable cybersecurity community and ecosystem.

[1] https://www.nsf.gov/about/budget/fy2012/pdf/40_fy2012.pdf

About CTSC's Fourth Year

CTSC project year four (October 1, 2015 - September 30, 2016) represented a no-cost extension on the CTSC grant. The majority of the remaining funds was spent by the end of calendar year 2015 and the majority of the activities in this report occurred during that period. Two partners (University of Wisconsin and University of Wisconsin-Milwaukee) had funding that carried over into 2016, allowing some activity to occur throughout the project year. While this report stands on its own, a reader will obtain valuable context from CTSC's Year Three Report[2].

In late 2016, the project team was informed by NSF that a proposal they had submitted to the Cybersecurity Innovation for Cyberinfrastructure (CICI)[3] for a NSF Cybersecurity Center of Excellence was to be awarded. The fourth year hence included planning for a clean transition to this critical new award.

CTSC Impact on the NSF Community

In this section, we present key metrics summarizing the impact of CTSC's activities on the NSF community over its first four years. Subsequent sections of this report describe the fourth year activities in detail.

Method of Impact	**Total # of NSF Projects & Facilities**	**Total # of NSF Large Facilities**	**Total # of NSF Personnel**
One-on-one engagements (completed and in progress)	22	7	n/a
Training	74 individuals representing 63 projects	33 individuals representing 15 Large Facilities	15
Cybersecurity Summit Attendance	111	15	34

Table 1: NSF projects and personnel directly impacted by CTSC

[2] http://hdl.handle.net/2022/20401

[3] https://www.nsf.gov/pubs/2015/nsf15549/nsf15549.htm

Metric	Value
Training curriculum developed	5[4]
Training sessions provided	20
Number of in-person trainees	294
Online training videos	33
Number of views for online training	6,369
Number of individuals attending one or more cybersecurity summits	186
Number of views of blog posts (best practices, guidance)	13,990
Unique visitors to trustedci.org website	2,664
Number of technical reports, guidance publications, and published engagement products	41
Mentions in media, blog posts, etc.	2
Listed as a resource in an NSF solicitation	1
Invited talks	9

Table 2: Other CTSC impact metrics

Year Four Engagements

One of CTSC's main activities is an ongoing set of engagements with NSF-funded scientific CI projects to solve cybersecurity challenges faced by those projects. During the fourth year, CTSC undertook new engagements with the Gemini Observatory, PerfSonar, SciGaP, the Authentication and Authorisation for Research and Collaboration, and the Array of Things. Additionally planning for an engagement with MI-OSiRIS was undertaken. In this section we describe each of the engagements in turn, including the resulting benefits for the engaged projects and the broader scientific community. The following engagements were undertaken in year four. Some represent engagements started in year three. Some engagements were transitioned to the subsequently-funded NSF Cybersecurity of Excellence to complete.

SciGaP

The CTSC and SciGaP[5] teams had their final face-to-face meeting on December 17-18, 2015. Two reports: *Final Technical Recommendations* [SciGaP-FTR] and an *Engagement Summary* [SciGaP-Sum] captured what was learned and recommended during the course of the engagement. Additional reports and papers are listed at http://trustedci.org/scigap/.

Gemini Observatory

In October 2015, Gemini Observatory[6] and CTSC commenced an in-depth engagement

[4] Does not include advancement of the Secure Coding tutorial developed by Prof. Miller prior to CTSC's inception and revisions of the Cybersecurity Program development.

[5] http://scigap.org/

[6] http://www.gemini.edu/

as a follow-on from the brief "cybercheckup"-style engagement in June 2015. 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 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[7]. Gemini developed a priority task list and timeline for the development/revision and implementation of these and additional policies.

In November 2015, 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 Mauna Kea 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. CTSC ended its activities with Gemini at the end of 2015 and transferred the completion of the engagement to the NSF Cybersecurity Center of Excellence.

perfSONAR

perfSONAR[8] provides an appliance solution for running network tests across multiple domains. It is used extensively by the network research and education community, including numerous NSF CC-NIE awardees, with over 1300 deployments as of February 2015. Due to the complexity of the perfSONAR project, CTSC and perfSONAR undertook two engagements in parallel: one team addressing perfSONAR vulnerability management practices and the other reviewing perfSONAR source code for security weaknesses.

perfSONAR Vulnerability Management Practices Review

CTSC's team worked with perfSONAR to form a plan to implement the set of recommendations CTSC provided earlier in the engagement to help perfSONAR improve its user communication regarding maintenance and security updates of perfSONAR nodes. We also reviewed perfSONAR's current vulnerability management process with multiple members of perfSONAR team, and provided a set of recommendations for

[7] http://trustedci.org/guide
[8] http://www.perfsonar.net/

improving that process though more consistent handling, better communication with third-party reporters and perfSONAR node operators, and process automation and simplification. In the process of these tasks, CTSC team members discovered specific vulnerabilities within the node design and configuration, which were communicated to the perfSONAR team along with severity estimates.

perfSONAR Code Review

Work on the perfSONAR Code Review of BWCTL concluded in October-November 2015. A final report [perfSONAR-CR] was completed in December and approved by the perfSONAR team on January 6, 2016.

AARC

The two-year Authentication and Authorisation for Research and Collaboration (AARC) project[9] started in May 2015 to "develop an integrated cross-discipline AAI framework, built on production and existing federated access services."[10] The project team consists of 20 European partners, lead by the former Trans-European Research and Education Networking Association (TERENA) now known as GÉANT.

During a presentation about AARC at the Federated Identity Management for Research Collaborations (FIM4R) meeting[11] in February 2015, attendees discussed the importance of coordinating AARC activities with representatives of US research cyberinfrastructure. As a result, CTSC established an engagement with AARC to gather input from US cyberinfrastructure projects on AARC-lead activities, disseminate training and other AARC project outputs to US cyberinfrastructure projects, and facilitate EU-US pilot project activities.

AARC engagement activities during the NCE period included active participation in the following meetings:

- Federated identity and incident response sessions at the Internet2 Tech Exchange meeting[12] in October 2015.
- Workshop on Information Security for collaborating E-infrastructures[13] in October 2015.
- AARC training workshop[14] in October 2015.
- REFEDS, eduGAIN, and FIM4R sessions[15] at the European Workshop on Trust & Identity (EWTI) in December 2015.

MI-OSiRIS

The Multi-Institutional Open Storage Research InfraStructure (MI-OSiRIS) project,

[9] https://aarc-project.eu/
[10] https://aarc-project.eu/about/
[11] https://indico.cern.ch/event/358127/
[12] https://meetings.internet2.edu/2015-technology-exchange/
[13] https://www.terena.org/activities/ism/wise-ws/
[14] https://eventr.terena.org/events/2240
[15] https://eventr.terena.org/events/2188

funded under the NSF CC*DNI DIBBs program (award #1541335), is developing a storage architecture based on the Ceph data management system to support multi-institutional collaboration on large data. CTSC staff met with MI-OSiRIS project staff in October and November 2015 to begin planning for an engagement focused on identity and credential management challenges. The engagement is expected to launch during Y1 of the Cybersecurity Center of Excellence.

Array of Things

The Array of Things[16] (AoT) is an NSF-funded urban sensing project, a network of hundreds of interactive, modular sensor boxes that will be installed around Chicago to collect real-time data on the city's environment, infrastructure, and activity for research and public use. This initiative has the potential to allow researchers, policymakers, developers, and residents to work together to evaluate and take specific actions that will make Chicago and other cities healthier, more efficient, and more livable.

During the NCE, CTSC disseminated the findings regarding privacy at the Streams2015 workshop [AoT] and planned for an engagement with the AoT project by the NSF Cybersecurity Center of Excellence.

Education, Outreach and Training

A key component of our mission to achieve more trustworthy NSF scientific CI is the development of new cybersecurity expertise through the creation, dissemination, and delivery of training and educational materials, and outreach to the community to make them aware of CTSC's services and improve the understanding of cybersecurity for science. Towards this end, CTSC undertakes a set of Education, Outreach and Training (EOT) activities.

Training

CTSC provided training in Automated Software Assessment Tools at the International Conference on Software Engineering and Data Engineering, San Diego, Calif., October 2015[17].

Outreach

CTSC undertakes outreach activities both to disseminate its work and to make NSF CI projects aware of its services. CTSC's outreach mechanisms include the CTSC website (trustedci.org), an ongoing blog covering CTSC's activities (blog.trustedci.org), and a Twitter account to disseminate both the CTSC blog posts and other cybersecurity news of interest to NSF CI projects (twitter.com/trustedci). CTSC presentations in Year four were:

- Von Welch. Cybersecurity for Trustworthy Science. IU Booth Presentation at SC15, November 2015. https://dx.doi.org/10.6084/m9.figshare.3118132
- Von Welch. Update on IdM for Research. MAGIC Meeting co-located with SC15,

[16] arrayofthings.us

[17] https://www.cse.unr.edu/SEDE/

November 2015. https://dx.doi.org/10.6084/m9.figshare.3118135

- Von Welch. Cybersecurity for Science: Risk Management-based Approach from the Center for Trustworthy Scientific Cyberinfrastructure. Lecture notes for presentation to Information Security Law, B587 class, November 2015. http://dx.doi.org/10.6084/m9.figshare.1597726
- Bob Cowles. CTSC Guide to Developing Cybersecurity Programs for Science and Engineering Project. WISE Workshop, Barcelona. October 2015. https://www.terena.org/activities/ism/wise-ws/slides/CTSC-WISE-Oct-2015.pdf
- Von Welch. Urban Sensor Data Privacy Issues: Findings of the Array of Things (AoT) Privacy Breakout Group. Presentation at STREAM 2015 Workshop, October 2015. http://dx.doi.org/10.6084/m9.figshare.1591205

Additionally, CTSC staff attended a NSF-funded Cybersecurity Technology Transfer to Practice Workshop[18] to discuss security issues around sustainability.

Leadership of NSF CI Cybersecurity

A key challenge for CTSC is being responsive to community needs, while also staying ahead of emerging problems and providing leadership in addressing them. Over the course of its day-to-day activities, CTSC needs to lead the community towards a coherent, interoperable cybersecurity ecosystem while serving each individual project well. CTSC will leverage a broad understanding of the NSF CI community to actively seek opportunities to align cybersecurity solutions for interoperability to better support collaboration.

NSF Cybersecurity Summit

During year three, CTSC hosted the 2015 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure. In January of 2016, CTSC published the report from the 2015 Summit[19]

CTSC Cybersecurity Program

Work on CTSC's Cybersecurity Program was not completed as planned because of the completed spend down of funds at PSC/CMU early in year 4. It was started and then prepared for transition to the Cybersecurity Center of Excellence.

CTSC Collaborations

During year four, CTSC maintained its strong collaborations with the NSF-funded Bro Center of Expertise[20], Internet2, the Department of Energy, the DHS-funded SWAMP project[21], and the REN-ISAC[22]. CTSC coordinated with these partners to foster a transition from CTSC to the NSF Cybersecurity Center of Excellence.

---

[18] http://www.southalabama.edu/colleges/soc/research/ttp/ttpworkshop2.html
[19] https://scholarworks.iu.edu/dspace/handle/2022/20539
[20] https://www.bro.org/nsf/
[21] https://continuousassurance.org/
[22] http://www.ren-isac.net/

CTSC Advisory Committee

To make sure CTSC is well aligned with the needs of the NSF CI community, and in touch with the broader CI and cybersecurity communities, it is guided by an advisory committee. The committee was formed at the start of the project and meets twice a year, remotely in May (via teleconference) and in-person in November (co-located with the Supercomputing conference[23]).

The CTSC advisory committee members are:

- Tom Barton is senior director for architecture, integration and chief information security officer at the University of Chicago.
- Neil Chue Hong is director of the Software Sustainability Institute (SSI), the UK national facility for cultivating world-class research through software.
- Don E. Middleton leads the Visualization and Enabling Technologies Section in NCAR's Computational and Information Systems Laboratory and currently serves as PI or co-PI on a number of projects, including the Earth System Grid, the Earth System Curator, the Virtual Solar Terrestrial Observatory, the North American Regional Climate Change Assessment Program, the Cooperative Arctic Data and Information Service, and NCAR's Cyberinfrastructure Strategic Initiative.
- Nicholas J. Multari is the senior project manager for research in cybersecurity at the Pacific Northwest National Lab (PNNL) in Richland, Washington.
- Nancy Wilkins-Diehr of the San Diego Supercomputing Center has a breadth of experience in community engagement. She is currently director of XSEDE's Extended Collaborative Support for Communities program, which includes Science Gateway initiatives. She is also the PI on a Science Gateway Institute conceptualization grant.

For full bios, please see http://trustedci.org/advisory-committee/.

During year four, CTSC organized and hosted a meeting of the advisory committee on November 19th in Austin, co-located with SuperComputing'15. The meeting was used to present plans for a transition to the NSF Cybersecurity Center of Excellence and receive feedback.

Lessons Learned

CTSC continues to evolve and refine the following lessons learned, as first reported in its year one report. The order is not meaningful.

Engagements are Essential

In addition to direct impact, CTSC's direct, typically one-on-one, engagements with NSF projects have proven essential for CTSC's maturation. While CTSC consists of cybersecurity professionals who have undertaken many risk assessments and developed numerous cybersecurity plans over their careers, engagements provide an opportunity to perform those tasks with a frequency and with a breadth of projects that would typically

[23] http://supercomputing.org/

be impossible. This work provides an opportunity to experiment with different techniques and determine which approaches best serve the broader NSF CI community. It also keeps CTSC involved "on the ground" and prevents the project's work from veering toward the purely theoretical. We find that having at least one in-person meeting early in an engagement is critical to establishing effective teamwork.

Engagements Require Flexibility and Innovation

Having completed nearly two dozen engagements, CTSC has begun to discern the factors that substantially impact the best form for an engagement, including the following:

- at what point is the project in its lifecycle;
- is the project focused on a specific scientific problem or domain, or is it providing general purpose infrastructure;
- is the project developing software, operating infrastructure, or both;
- does the project have an existing cybersecurity program;
- how large and complex is the project; and
- the perceived understanding and support of cybersecurity by project leadership.

CTSC has learned to try different engagement models (e.g., peer reviews, "cyber checkups") in order to adapt to different types of projects. As these models prove useful, we then work to institutionalize them in CTSC with well-defined processes so we can execute them efficiently.

Even when a project and engagement approach is well understood, unexpected events (e.g., events that require the engaged project to re-prioritize temporarily) require flexibility in managing the engagement. To adapt to unexpected events, we recognize that our engagement teams will sometimes have spare effort due to being blocked, as well as the need for additional effort. To allow for flexibility, CTSC maintains an ongoing task to develop training materials, best practices and other deliverables with flexible deadlines. This allows staff to be applied to or from those deliverables and time-sensitive engagement tasks.

Engagements Red Flags in Terms of Lasting Impact

Over the course of nearly two dozen engagements, CTSC has begun to discern the factors that are concerns for the engagement having a deep, sustained impact, including the following:

- The project management failing to agree and commit to an engagement plan. CTSC has found lack of strong commitment by management to be sufficient problem that we no longer will begin the work of an engagement without a mutually agreed-to plan.
- A lack of dedicated resources and/or cybersecurity budget by projects. While CTSC don't have a firm test for this, it is recognized that projects cannot simply put resources towards cybersecurity during an engagement with CTSC without long-term commitment. CTSC plans on asking about cybersecurity budgetarily in the future and consider this in our assessment for long-term impact.
- The presence of strongly competing priorities. While CTSC recognizes that it will

be rare for a project not to have other tasks they are focused on during an engagement, there are times during a project lifecycle during which the potential for distraction, and hence a lack of participation in an engagement is increased - e.g. right before a initial release. CTSC should try to discern this risk and manage it appropriately by, e.g., focusing tightly or delaying an engagement.

- A lack of application of basic cybersecurity hygiene. While it is true that scientific projects have unusual risks that basic cybersecurity hygiene (e.g., SANS Top 20, CTSC Guide to Securing Commodity IT) does not address well, CTSC has determined applying such basic hygiene is a good foundation for nearly any project that has some commodity IT infrastructure. CTSC should consider if a project applying for an engagement has applied a base hygiene program and either suggest it as a predicate to engagement or the goal of an initially tightly focused engagement.

The Summit is Critical to Community Building and Outreach

CTSC has now hosted three 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. Relationships formed at and around the summits have resulted in several of CTSC's engagements. As discussed in the following lessons, the summits have also been a valuable venue for CTSC to deliver training.

Venues for Delivering Training are Scarce

There are not many venues that offer opportunities either to provide or receive cybersecurity training targeted to the needs of our community. Many venues face a challenge in making time for specialized topics such as cybersecurity. While CTSC has had some success with Supercomputing and XSEDE (primarily with Secure Coding), the Summit remains the main venue for CTSC delivering training.

The training at the Summit and other venues has been well received. This leads to the consideration that an event for delivering training to CI professionals by CTSC and other projects across a range of specialized topics (e.g., data management, software engineering) could be well received by the community.

Templates Partially Address the Sharing Challenge

CTSC seeks to have as broad an impact as possible by sharing the work products of its engagements with the whole NSF CI community. However, projects are sometimes reluctant to allow this. We have had some success in the past year with the paradigm of developing a project-neutral template to address a relevant cybersecurity issue and then using that to complete the engagement objectives with a project. A template, while not a complete replacement for example cybersecurity plans, does serve as a valuable, easily shared resource.

Leveraging Campuses is Possible to a Degree

Every NSF CI project with which we have worked is embedded in and leverages varying

degrees of the commodity IT infrastructure, cybersecurity infrastructure and cybersecurity policies of the university or organization that hosts it. CTSC has been trying to answer the questions regarding the degree and circumstances in which projects can leverage this existing campus policy and infrastructure. While still not completely understood, some facets of the answers are starting to emerge:

- Commodity services such as vulnerability scanning and licenses for static analysis tools are sufficiently generic to be readily used by projects.
- Campus security offices tend to understand compliance-based security, so a project with HIPAA-covered data or social security numbers will likely find policies or infrastructure they can leverage.
- Due in part to the NSF CC-NIE/IIE program, networks tuned for science (e.g., Science DMZs) are increasingly available and may be of benefit to projects with large data movement needs.
- In general, campuses are not well positioned to provide comprehensive information security plans and programs for complex, large scale, often multi-institutional science projects.

Cyberinfrastructure has Its Own Security Challenges

In applying best practices from the broader cybersecurity community (e.g., NIST), CTSC continues to identify challenges specific to the NSF CI community, from unique assets such as scientific data and instruments, to challenges such as a close relationship to institutions of higher education and research. In particular, CI has a threat model which is not clear at this point given the community's unique assets and complex institutional and infrastructural relationships. A common misconception that CTSC witnesses is projects that have no data confidentiality requirements assume this means they have no need for cybersecurity. Counters to this assumption are that project data may still have integrity requirements, their project reputation could be hard by compromises to the point it impacts the reputation of their science, and their infrastructure could be used to attack others.

Strong Community Ties, Operational Security Expertise, and Diverse Backgrounds Critical to Success

Since its inception, the CTSC team has represented a wealth of operation security experience, strong connections to NSF and other major science projects, and a variety of practical experiences in related domains (e.g., law, risk management) and communities (e.g., software development, scientific, military, corporate, government). With three years behind us, these differing connections and backgrounds have proven invaluable in being able to initiate and establish relationships needed to form engagements with diverse scientific communities represented by different NSF projects, as well as bring broader information security best practices to bear.

Conclusion

This report covers CTSC's final fourth year under a no-cost extension. This year represented only a partial year of effort for the project due to the exhaustion of the

majority of the funding by three months into the year. CTSC focused its efforts on completing engagements, publishing the 2015 NSF Cybersecurity Summit Report, and preparing to transition its work to a newly-funded NSF Cybersecurity Center of Excellence.

Over its four years, CTSC's impact on the NSF CI community has been impressive, with over 180 individuals, representing over 110 projects, attending one of three Summits, over nearly 300 CI professionals representing over 60 projects attending CTSC-led training. Those numbers include a significant impact on NSF Large Facilities, who comprised 7 CTSC engagees, 15 of the projects who have attended a Summit and benefitted from CTSC training. Seven students were exposed to cybersecurity and NSF science, two working directly with CTSC for multiple months. CTSC outreach through presentations, social media, publications, and leadership in InCommon broadly informed and impacted the community.

References

- [2016Summit] Jackson, C., Marsteller, J., Starzynski Coddens, A., and Welch, V., *Report of the 2015 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure*. January, 2016. http://hdl.handle.net/2022/20539
- [AoT] Welch, V., and Catlett, C.. *Urban Sensor Data Privacy Issues: Findings of the Array of Things (AoT) Privacy Breakout Group.* Streams2015, October 2015. https://dx.doi.org/10.6084/m9.figshare.3117172
- [perfSONAR-CR] Heiland, R., Adams, A., Heymann, E. *perfSONAR-CTSC Code Review Engagement Final Report*. CTSC Engagement Report. http://hdl.handle.net/2022/20596
- [S3I2] Butler, R., V. Welch, J. Basney, S. Koranda, W.K. Barnett and D. Pearson. Report of NSF Workshop Series on Scientific Software Security Innovation Institute. 2011. Available from: http://hdl.handle.net/2022/14174 [cited 12 Feb 2012]
- [SciGaP-FTR] Heiland, R., Koranda, S., Welch, V. *SciGaP-CTSC Engagement: Final Technical Recommendations*. CTSC Engagement Report. http://hdl.handle.net/2022/20927
- [SciGaP-Sum] Heiland, R., Koranda, S., Welch, V. *SciGaP-CTSC Engagement Summary*. CTSC Engagement Report. http://hdl.handle.net/2022/20926