Center for Trustworthy Scientific Cyberinfrastructure

Year Two Report

NSF ACI Grant # 1234408
Covering Project Year 2
October 1, 2013 - September 30, 2014

CTSC Team

Jared Allar[1], Jim Basney[3] (co-PI), Rakesh Bobba[3], Randy Butler[3] (co-PI), Patrick Duda[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], Von Welch[2] (PI)

CTSC Students

Betsy Thomas[2], Epaphras Matsangaise[2]

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

About CTSC

The mission of the Center for Trustworthy Scientific Cyberinfrastructure (CTSC, trustedci.org) is to improve the cybersecurity of NSF science and engineering projects, while allowing those projects to focus on their science endeavors. This mission is accomplished through one-on-one engagements with projects to address their specific challenges; education, outreach, and training to raise the state of security practice across the scientific enterprise; and leadership on bringing the best and most relevant cybersecurity research to bear on the NSF cyberinfrastructure research community. For more information about the Center for Trustworthy Scientific Cyberinfrastructure please visit: http://trustedci.org/

Acknowledgments

CTSC is 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 author(s) and do not necessarily reflect the views of the National Science Foundation.

Using & Citing this Work

Table of Contents

1. Executive Summary

The Center for Trustworthy Scientific Cyberinfrastructure (CTSC) is transforming and improving the practice of cybersecurity and hence the trustworthiness of NSF scientific cyberinfrastructure (CI). CTSC is providing 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; 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 two, from October 2013 through September 2014, during which time CTSC engaged with seven NSF CI projects; re-invigorated the NSF CI cybersecurity community by organizing the 2013 and 2014 NSF Cybersecurity Summits for Large Facilities and Cyberinfrastructure; provided the community with a guide and templates for developing a cybersecurity program; and provided training in secure coding, incident response, and developing a cybersecurity program.

Nearly 150 individuals, representing over 70 projects, attended one or both of the NSF Cybersecurity Summits. The 2014 Summit was particularly successful in building the community around a call for participation that resulted in the broader community presenting two training sessions and four experience reports.

Through its first two years, CTSC has now engaged with 13 NSF projects, and trained over 130 CI professionals representing 30 projects. Those numbers include a significant impact on NSF Large Facilities, 4 of which are CTSC engagees. Additionally, individuals from 14 of the engaged projects have attended a Summit, and 9 of the engaged projects benefitted from CTSC training.

Awareness of CTSC increased in its second year, with *International Science Grid This Week* publishing an article on CTSC's work with LIGO, an NSF solicitation mentioning the CTSC-organized Summit, and CTSC's blog and website receiving a significant number of views.

This report describes all of CTSC's second year activities in detail, concluding with a set of lessons learned by CTSC over its first two years, as well as the project's plans for its third year.

2. Introduction: CTSC Overview and Vision

The Center for Trustworthy Scientific Cyberinfrastructure (CTSC) is transforming and improving the practice of cybersecurity and hence trustworthiness of NSF scientific cyberinfrastructure (CI) and the science it enables. CTSC is providing 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, and the annual NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure.

As NSF pushes toward 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 strong cybersecurity measures. Projects are forced to divert their resources to develop appropriate expertise; tend to address risks haphazardly and unknowingly reinvent basic cybersecurity solutions; and struggle with interoperability [S3I2]. Contributing to the challenge is the fact that cybersecurity cannot be 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, all of which make 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 indiscriminately between projects and 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 within a coherent cybersecurity ecosystem; has access to the tools and expertise to enact a cybersecurity program; 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 undertakes 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

3. 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 two years. Subsequent sections of this report describe the activities in detail.

Table 1: CTSC impact metrics

Metric	**Value**
Training curriculum developed	3[2]
Training sessions provided	14
Number of in-person trainees	242
Online training videos	19
Number of views for online training	707
Number of individuals attending one or both cybersecurity summits	148
Number of views of blog posts (best practices, guidance)	12,022
Unique visitors to trustedci.org website	2,281
Number of technical reports, guidance publications, and published engagement products	25
Mentions in media, blog posts, etc.	2
Listed as a resource in an NSF solicitation	1
Invited talks	6

[2] Does not include advancement of the Secure Coding tutorial developed by Prof. Miller prior to CTSC's inception and a revision of the Cybersecurity Program development in year two.

Table 2: NSF projects and personnel directly impacted by CTSC

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)	13	4	n/a
Training	39 individuals representing 30 projects	19 individuals representing 12 Large Facilities	9
Cybersecurity Summit Attendance	71	14	20

4. 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 second year, CTSC undertook engagements with the Daniel K. Inouye Solar Telescope (DKIST, formerly the Advanced Technology Solar Telescope, ATST), Science Gateways Platforms as a Service (SciGaP), Globus, HUBzero, Sustainable Environmental Actionable Data (SEAD), Large Synoptic Survey Telescope (LSST), and orchestrated a peer review between two CC-NIE projects at Penn State University and the University of Utah.

The latter peer review represented CTSC's pioneering new methods for engagement to scale our services to NSF programs with a large number of projects that would otherwise prohibit our direct engagement with even a large fraction thereof (the CC-NIE program, including awardees in 2014, will have over 100 projects). Another example of CTSC's experimentation is our development and execution of a "CyberCheckup," a week-long process to identify gaps in an established cybersecurity program, which we implemented in our engagement with HUBzero.

In this section we describe each of the engagements in turn, including the resulting benefits for the engaged projects and the broader scientific community. Importantly, all CTSC engagement plans call for follow-up contact with engagement communities to assess the impact of the engagements. For all of the listed current engagements, as well as engagements completed in year one, we solicited and included a statement from the project regarding the engagement and its impact. Comments from the projects are included verbatim with no modification by CTSC.

5. Year Two Engagements

The following engagements were undertaken or completed in year two.

5.1 DKIST and a Guide for NSF Science and Engineering Projects

The Daniel K. Inouye Solar Telescope (DKIST) (f.k.a. Advanced Technology Solar Telescope or ATST) is an NSF-funded Major Research Equipment and Facilities Construction (MREFC) project whose construction began in 2010 and is planned to be completed in 2017. The DKIST will be the largest solar telescope in the world and will be located in Haleakalā, Hawai'i with an operations center in Boulder, Colorado. At the 2013 NSF Cybersecurity Summit, Bret Goodrich, Senior Software Engineer for DKIST, approached CTSC staff to discuss how to develop a cybersecurity program for cyberinfrastructure projects. As an NSF MREFC project, DKIST had a requirement to develop a cybersecurity program plan in keeping with the NSF Cooperative Agreement Supplemental Financial & Administrative Terms and Conditions on information security.[3]

The primary goal of the engagement was to enable the development of a cybersecurity program for DKIST. Unlike other similar engagements, the end product of the engagement was not DKIST's cybersecurity program plan itself, but instead, to provide DKIST with a set of artifacts and knowledge that would leave DKIST in a position where it could complete such a plan on its own timeline. With this goal in mind, CTSC undertook the development of a Cybersecurity Planning Guide for CI projects, including supporting policy and process templates designed to assist DKIST and other NSF cyberinfrastructure projects in developing their own cybersecurity programs.

In October of 2013, CTSC and DKIST began drafting a guide on conducting a risk-based approach to developing cybersecurity programs. The team used a number of resources including the standard NIST 800-30 framework and the experience of earlier risk assessments performed by NCSA and PSC for other NSF projects including Blue Waters, XSEDE, and GENI.

In order to meet the needs of the CI community, a set of challenges were identified:

- Risk assessments can represent significant undertakings, requiring more resource hours to complete than CTSC felt could be expected from smaller scale NSF CI project teams.
- Addressing unusual and even unique scientific instruments and data.
- Unusual requirements of the science community, such as the need for privacy of pre-publication data and concerns about data integrity that might bring science results into question.
- Efficiently addressing the fact most CI projects are embedded in one or more organizations

[3] http://www.nsf.gov/pubs/policydocs/cafatc/cafatc_ffrdc212.pdf (Article 59)

(typically universities or research laboratories) and benefit from, and likewise are restricted by, the cybersecurity programs and commodity IT infrastructure of those organizations.

Over the course of nine months the CTSC team applied the knowledge and experience gained from past engagements along the CI perspective as well as contributions from DKIST to develop the first cybersecurity planning guide specifically for our community.

CTSC has been honing the process used in the previously mentioned risk assessments to be more streamlined and easily repeatable, with a set of common threats and types of assets for CI projects, and methods for abstracting the complicated relationships within their underlying organizations.

In August of 2014 CTSC published Version 1 of the "Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects" on the CTSC website.[4] Accompanying the guide are over 15 supporting documents including policy templates, risk assessment tools, training and awareness resources, commodity IT best practices and operational security resources. This effort represents the most comprehensive set of CI-focused cybersecurity tools available that can be applied to NSF funded projects to advance the state of cybersecurity practice and improve program consistency.

While initially developed for the DKIST engagement, we expect to keep improving this approach throughout the life of CTSC by applying it to new projects and seeking additional input from the CI community.

To promote the guide, CTSC held a half-day tutorial at the 2014 NSF Cybersecurity Summit in Arlington, VA. Response to the training session was very strong with 86% of those attending rating the session as "very useful" or "extremely useful". Some of the comments from training attendees include:

- *"I thought the templates were very helpful. It was also important to see a focus on a risk-based approach. The whole session was very, very good."*
- *"I think the level of detail was very good and very informative for the Developing Cybersecurity Programs for NSF projects"*
- *"Provided templates are excellent!"*

Bret Goodrich was invited to participate on the "Large Facilities' Cybersecurity Challenges and Successes" session at the cybersecurity summit to share his experience over the past year working with CTSC to develop a cybersecurity program. In introducing himself to the other panelists he summarized his experience:

> *"As a person who stepped off that virtual cliff in 2013, I can speak about how far I've come from the last summit. In the last year, my project has developed an outline for meeting the NSF*

[4] http://trustedci.org/guide

requirements. I am now working toward implementing a plan (we need to actually build the facility first!) but I now have schedule and budget allocated to address cybersecurity infrastructure, a set of requirements for the protection of our facility, and probably most importantly to me, a senior management that has been educated on what we need and why we need it.

I hope I can help on the panel as that new person who did take up the challenge of last year's summit. I am more than happy to discuss how far we've come-and how much further remains."

5.2 Globus

In September of 2013, CTSC began an engagement with the Globus (formerly Globus Online)[5] team at the Argonne National Laboratory and University of Chicago. The Globus flagship service provides file transfer service with the goal of providing ease and reliability to its users. Recently the Globus team added functionality to support file sharing, i.e. "big data sharing and transfer with Dropbox-like simplicity."[6]

The primary focus of the CTSC/Globus engagement was to conduct a cybersecurity review of the architecture and design of the new sharing functionality. After an initial call to kick off the engagement, the Globus team collected and prepared design and architecture documentation to share with CTSC staff to aid in the formal construction of the engagement plan. CTSC staff then deployed instances of the Globus Connect Server[7] (a bundling of the Globus GridFTP Server, MyProxy Server, Simple CA, and new wrapper scripts, etc.) and exercised a number of sharing scenarios to understand the capabilities of the sharing feature as well as the workflows that Globus users and resource administrators would experience when deploying the necessary tools while both sharing and consuming shared resources (files). While the engagement did not include a complete code review, the code for some of the newer enhancements to the GridFTP Server that make the sharing functionality possible was examined to better understand from first principles the details of how the sharing functionality is implemented at the resource host site.

During the course of the assessment the Globus team made available to CTSC an assessment document prepared by staff at the San Diego Supercomputing Center (SDSC). Globus asked that the CTSC assessment not dwell on issues found by SDSC since the Globus team had already decided to implement changes requested by SDSC as a result of the SDSC assessment. CTSC staff studied the SDSC assessment and incorporated it into the assessment process. Additionally, CTSC was provided with an assessment by

---

[5] https://www.globus.org/ - funded by NSF SI2 and supporting a variety of users, see https://www.globus.org/case-studies

[6] Private communication with the Globus team.

[7] https://support.globus.org/entries/23857088

an XSEDE team that was also charged with assessing the Globus sharing functionality within the context of possible XSEDE support for sharing. That assessment provided context and helped inform the CTSC assessment. We view the cooperation between CTSC, SDSC, and XSEDE and the sharing of assessment criteria and outcomes as a strong indicator of the successful community building that is occurring in terms of cyberinfrastructure in support of research and education.

CTSC staff then developed a set of review principles that formed the foundation for the basis of the assessment. The following principles were used for the assessment and are based on those put forth by Saltzer and Schroeder [Saltzer1975], and Saltzer and Kaashoek [Saltzer2009], with strong influence from Smith [Smith2012]. The principles were further shaped by the experience of the reviewers and CTSC staff:

1. Open Design
2. Minimize Secrets
3. Defined Trust and Authority Model
4. Transparency
5. Fail-safe Defaults
6. Principle of Least Astonishment
7. Least Privilege
8. Lifecycle Management
9. Coherency Management

Using the above principles to shape the assessment, and based on both the Globus sharing documentation provided by Globus and the experience of deploying the server and exercising various sharing workflows, CTSC staff prepared 22 recommendations for the Globus team. Here we list a few illustrative samples of recommendations:

- Open Design: The code responsible for receiving and then processing the USER:globus-sharing:, SITE SHARING, and SITE RESTRICT commands should be independently audited since it implements new functionality not previously used in Globus GridFTP deployments.
- Transparency: Globus should allow RP administrators to be notified when shares are created on their resources.
- Transparency: Additional logging capabilities should be added to the GridFTP server to allow configuration by an administrator to log the full details of all credentials (including all certificates in a chain both for sharing and non-sharing access) used when a client accesses the server.
- Least Privilege: It should not be possible to create a share such that the configuration for sharing could be modified via the share.
- Lifecycle Management: Shares should have a lifespan so that they need to be periodically (annually seems like a reasonable default) verified by the creating user as valid.

The CTSC assessment has been delivered to the Globus team and CTSC is awaiting feedback.

5.3 HUBzero

As described on their website[8], HUBzero is an open source software platform for building powerful web sites, or "hubs" that support scientific discovery, learning, and collaboration. HUBzero was originally created by researchers at Purdue University in conjunction with the NSF-sponsored Network for Computational Nanotechnology to support nanoHUB.org. The HUBzero platform now supports dozens of hubs across a variety of disciplines, including cancer research, pharmaceuticals, biofuels, microelectromechanical systems, climate modeling, water quality, volcanology, and more.

In April 2014, CTSC conducted a "CyberCheckup" for HUBzero, an example of CTSC's innovating new engagement methods. This method is a short, focused engagement that identifies gaps in an existing cybersecurity program. CTSC staff reviewed 6 HUBzero documents and produced a 2 page report for HUBzero staff within the one week CyberCheckup period. CTSC staff used a checklist of baseline controls and best practices to identify topics to cover during the CyberCheckup.

CTSC's broader engagement with HUBzero kicked off in September with a close review of their Web Server Security Model and Disaster Recovery Plan documents. CTSC provided HUBzero with recommendations to improve upon their existing policy and procedures to better address issues of access control and incident response procedure.

The engagement is moving forward now with the development of a Content Management System (CMS) Access Control and Security Model to complement the Web Server Security Model. The process is both one of discovery – codifying ad-hoc practices into a document that can be analyzed and improved – and analysis with the goal of producing actionable recommendations. This allows HUBzero to get the largest return on their continuing efforts to secure their core software offering.

In parallel with the CMS Access Control and Security Model effort, the engagement is working to generate Vulnerability Management policies and procedures for both the operations of HUBzero's hosted hubs and the development of HUBzero's CMS software. In addition to policies and procedures addressing HUBzero's unique needs, this work is generating templates that can be applied by other projects in conjunction with the Cybersecurity Planning Guide developed during CTSC's engagement with DKIST.

Comment from Michael McLennan:

> *"HUBzero is an open source software platform used to by more than 60 communities to create science gateway web sites for many different research areas. Many of these sites have tens of thousands, or even hundreds of thousands, of users each year. Some sites support projects that require HIPAA or ITAR compliance. Cybersecurity is absolutely critical for all of the projects, so we are always looking for ways to*

[8] https://hubzero.org/ (much of this paragraph is quoted from that website)

improve our software and our hosting services.

The CTSC team started an engagement with HUBzero this past April. Their initial CyberCheckup gave us confidence that we are doing things well, but also pointed out a few things that we could improve, such as adding two-factor authentication for administrative access. We are now starting a deeper engagement that will help us find any gaps in the access control model of our content management system, and help us improve our policies for vulnerability management.

Even though we've just started, we've already formed a strong partnership. I am impressed with the expertise that the CTSC staff have in many different areas, including authentication, IT policy, and even law. Their approach to our engagement has been well-organized and professional. I look forward to working with them during the coming year to improve our cybersecurity."

5.4 SciGaP

The Science Gateways Platform as a Service (SciGaP[9]) is an NSF-funded collaborative project between Indiana University, the San Diego Supercomputing Center and the University of Texas Health Science Center with the goal of enabling scientific communities to utilize cyberinfrastructure by providing APIs to hosted generic infrastructure services. These services can then be easily adopted by gateway providers to build new gateways (and improve existing ones). Typical services will allow users to schedule and run jobs – perhaps within complex workflows – on computational resources. In order to do that securely, additional services that provide user authentication and authorization will be required.

Science gateways became part of the NSF-funded CI landscape around 2004 as part of the TeraGrid project. They have seen considerable growth [Wilkins-Diehr] since that time, both in the number of gateways and in the number of researchers using them. Gateway clients were initially envisioned to be web-based (a.k.a. portals) with easy-to-use interfaces in a browser. While web-based science gateway clients are still prevalent today, they also now include "native" clients: desktop applications, mobile apps, and scripts in a variety of languages that run outside of web browsers. The protocols used for client-server communication have also evolved. SOAP was often used in some of the early gateways, followed by REST (though not technically a protocol) which remains very popular. SciGaP will explore a

[9] http://www.scigap.org/ - funded by NSF ACI awards 1339774, 1339649, and 1339856

different approach by adopting Apache Thrift.[10] Thrift follows the remote procedure call (RPC) paradigm and can generate multi-language services from an interface definition language (IDL). Thrift also supports several different protocols and transport mechanisms; however, it is non-RESTful. It is Thrift's protocols and transports that are believed to be beneficial for the SciGaP project and the resulting science gateways, e.g. by providing a faster binary protocol and by making it easier to handle complex data structures. These same protocols and transports need a close security review and will be part of our engagement going forward.

Since SciGaP is still a relatively young project (it began in late 2013) and was in a "getting started" phase when CTSC initially engaged them, finding a good engagement model has been a bit challenging. Originally the engagement focused on a review of their architectural design and implementation of a "credential store," the functionality for securely authenticating and authorizing credentials for gateway users who would be executing SciGaP services. Since, the SciGaP project's design has evolved and its priorities have changed. The engagement then shifted to a review of issues related to the secure use of Thrift, a protocol framework used by Evernote among others. Our preliminary summary of the security practices for Thrift can be found at http://trustedci.org/scigap/.

A second area of engagement concerns recommendations for developing and ensuring more secure software for SciGaP, since it is very much in a software development phase. Although CTSC does not have the resources to do a full code walkthrough of the SciGaP software, we will suggest tools and services that can be used to perform analyses that check for vulnerabilities. For example, we uploaded an early version of the core SciGaP code base (Apache Airavata) to the Software Assurance Marketplace (SWAMP[11]) service (https://www.mir-swamp.org/) and performed a preliminary static analysis on that Java code.

Finally, a third area of engagement will be to offer recommendations on Identity Management (IdM). SciGaP has identified three use cases for managing user identities and CTSC has just begun discussing these with them. SciGaP has the challenge of needing to support both existing ("classic") and future science gateways, including those with native clients.

To accommodate the relatively early state of design of the SciGaP project, CTSC and SciGap are experimenting with a different engagement model. Essentially, this model will take on a longer timeframe (several months) with ongoing interaction and shorter-term engagement tasks. This contrasts with most of our other engagements, where longer-term tasks were defined early in the engagement.

---

[10] Thrift originally began as a project at Facebook before being donated as open source to the Apache Software Foundation.

[11] Disclosure: The CTSC PI and other teams members are also involved in the SWAMP project.

Initial feedback that we have received from the PI, Marlon Pierce, has been positive:

> *"The engagement has been useful so far and we appreciate CTSC's willingness to adapt their engagement model to our project. We also are planning to investigate the feasibility of Thrift over HTTPS based on CTSC's strong recommendation."*

5.5 CC-NIE Peer Review

The NSF CC-NIE (now CC-IIE) program[12] will have, with anticipated 2014 awards, over 100 projects, a number that CTSC cannot hope to engage with individually in any reasonable period of time. CTSC undertook a new form of engagement, dubbed a "peer review," with two CC-NIE projects with the goal of understanding how two projects could best interact to assess each other's cybersecurity programs. Projects at Penn State University[13] and the University of Utah[14] agreed to take part.

CTSC provided some initial guidance to the projects (see http://trustedci.org/cc-nie/), facilitated phone calls between the two projects and a member of the NSF-funded Bro Center of Expertise[15] to provide networking expertise, and authored the assessments based on the discussions between the participants. At the time of writing this report, assessments for both projects are in draft form.

While this engagement was an apparent success in terms of delivering assessments to both engagees, it was only a marginal success in terms of scaling. CTSC personnel spent about as much time on the peer review as they would have on an engagement with a single party, so a 2x improvement was obtained, but we do not believe the process will scale further by adding more participants since interactions were largely interactive between the two participants. To further improve scaling, CTSC would need to reduce its own involvement by providing better written guidance to the participants.

Comments from Joe Breen at the University of Utah on the peer review process:

> *"Over the summer of 2014, the CTSC facilitated meetings between the University of Utah and Penn State University to mutually review the security stance and security policy of the respective CC-NIE Science DMZ implementations. These meetings, with input from members of the Bro Project, yielded useful insights into the commonalities of security requirements, security approaches and security policies between the two institutions. These meetings also highlighted mutually useful and creative differences in approaches, i.e. the use of sFlow, Software Defined Networking, etc. that came about as products of different environments, both organizational*

---

[12] http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504748

[13] PI Agarwala, NSF award #1245980

[14] PI Corbato, NSF award #1341034

[15] https://www.bro.org/nsf/

and technical architecture. As the discussions iterated, common themes quickly bubbled to the top that both institutions noted were key to success:

Common themes key to success of the respective CC-NIE Science DMZ environments:

- *Tight collaboration of campus security, campus Network Operations, High Performance Computing facilities and the research community*
- *Campus governance process helping with the prioritization and alignment of key institution initiatives, research initiatives, and campus IT initiatives*
- *Security policy outlining the basic usage and access guidelines of the Science DMZ environments*
- *Process for working with "friendly" users and close collaborators at an early stage*
- *Availability and utilization of performance tools, specifically perfSONAR toolkit*
- *Availability and utilization of Science DMZ, performance and other documentation by groups such as ESnet, Internet2, peer institutions, etc. – particularly fasterdata.es.net*
- *Ability to support a Science DMZ high performance environment, AND, a prototype environment for new technologies, creative security and network approaches*

These common themes and the discussions regarding creative approaches to hard problems suggested possible future endeavors that the two institutions, CTSC and the Bro project might pursue with other institutions. Possible endeavors might be:

- *Community FAQ/Best Practices of implementing Science DMZ and security -- perhaps in conjunction with fasterdata.es.net?*
- *Knowledge base repository of approaches, architectures, security policies, etc. in a sanitized form that other institutions may leverage*

CTSC's facilitation, along with input from members of the Bro project, provided an excellent forum and set of circumstances for discussion and extrusion of these ideas between the two institutions. The discussion and ideas also emphasized the need (and gave the impetus) for bringing together various documents in a local campus repository of information."

6. Year One Engagements Updates

In this section we provide updates from CTSC engagements in project year one on longer-term impacts of their engagements.

6.1 LTER Network Office

The Long Term Ecological Research Network (LNO)[16] supports 26 sites and over 2000 scientists and graduate students with a long-term vision of "society in which long-term ecological knowledge contributes to the advancement of the health, productivity, and welfare of the global environment, thereby advancing human well-being."

The LNO engagement goal was to develop a risk-based cybersecurity plan. Specifically CTSC performed a risk assessment for the LNO Provenance Aware Synthesis Tracking Architecture (PASTA) data repository service, and then utilized that risk assessment to produce a cybersecurity plan for that service. LNO staff were engaged with us through the process so the transfer of the expertise from CTSC to LNO was also a part of this process.

Statement from James Brunt, LTER Network Office CIO, on ongoing impact from the CTSC engagement:

> *"In 2013 CTSC identified seven high priority risk mitigation issues for LNO. Of those seven five have been acted upon and responses to the other two have been limited by available resources. Two medium priority risk mitigation issues were identified and one is now being addressed. Five long-term goals and recommendations were provided and all except one of those recommendations are being addressed. It is important to note that the newly identified LNO Information Security Officer for the PASTA repository attended the CTSC sponsored Cyber Security Summit this year and he attended training both for Cyber Security Program Planning and for Incident Response Planning."*

6.2 LIGO

The Laser Interferometer Gravitational-Wave Observatory (LIGO) Scientific Collaboration[17] is a large research project funded by the National Science Foundation. LIGO seeks to make the first direct detection of gravitational waves, use them to explore the fundamental physics of gravity, and develop the emerging field of gravitational wave science as a tool of astronomical discovery.

---

[16] http://lternet.edu/ - funded by NSF BIO/DEB

[17] http://www.ligo.org/ - funded by NSF MPS/PHY

The primary goal of CTSC's LIGO engagement was to apply CTSC experience and expertise in leveraging SAML identity federations in order to remove barriers for efficient international collaboration between LIGO and other astronomy and astrophysics projects. Together CTSC and LIGO launched three simultaneous efforts to explore international SAML federation between LIGO and its collaborators. The three efforts were chosen to span the spectrum of federation approaches from point-to-point direct federation to bilateral federation agreements between existing large national SAML federations so that LIGO could (1) better understand the policy and technical issues surrounding international federation, (2) better understand the timelines necessary for each approach, and (3) begin to develop a long-term strategy for international interfederation in support of LIGO's long-term scientific mission.

As reported previously, the CTSC-LIGO engagement made concrete progress toward enabling international identity federation for collaboration between LIGO and other astronomy and astrophysics projects, blazing a trail for use of identity federation in other international scientific collaborations. The effort continues to bear fruit as evidenced by the recent announcement[18] by the InCommon federation. The announcement states that it has published SAML metadata for three service providers that support collaboration between LIGO and astronomers and astrophysicists from other projects into the eduGAIN[19] interfederation service. The publication of the three service providers into eduGAIN is a necessary step for providing interoperability between the service providers and applications and the identity providers or login servers used by scientists and researchers from around the world. Warren Anderson from the LIGO project writes:

> *"LIGO participates in a number of multi-messenger astronomy collaborations in which results from searches for gravitational waves are combined with astronomical observations of radio waves, visible light, x-rays, gamma-rays and neutrinos. These partnerships involve many more scientists from many more countries. A key tool of any scientific collaboration is an easily accessed and managed collaborative space. While national infrastructure, such as InCommon, is beginning to address the IAM needs of LIGO member institutions and their partners within national borders, this is insufficient for our needs. CTSC has enabled us to test internationally federated identity within LIGO...It will be central to LIGO and its collaborators to enable collaborative sharing with as few obstacles as possible going forward, and federated identity across as many international and institutional borders as possible will be the first step in enabling such collaboration. LIGO sincerely hopes that CTSC will play a lead role in enabling such agreements and infrastructure going forward."*

We note this work gained LIGO, CTSC, and InCommon some coverage in *International Science Grid this Week.*[20]

---

[18] https://spaces.internet2.edu/x/ZQ-kAg

[19] http://www.geant.net/service/eduGAIN/Pages/home.aspx

[20] http://www.isgtw.org/spotlight/federated-trust-expands-internationally-edugain-declaration

6.3 IceCube

The IceCube South Pole Neutrino Observatory[21] is a particle detector at the South Pole that records the interactions of a nearly massless subatomic particle called the neutrino. IceCube searches for neutrinos from the most violent astrophysical sources: events like exploding stars, gamma ray bursts, and cataclysmic phenomena involving black holes and neutron stars. The IceCube telescope is a powerful tool to search for dark matter, and could reveal the new physical processes associated with the enigmatic origin of the highest energy particles in nature. In addition to exploring the background of neutrinos produced in the atmosphere, IceCube studies the neutrinos themselves; their energies far exceed those produced by accelerator beams. IceCube is the world's largest neutrino detector, encompassing a cubic kilometer of ice.

The CTSC Team began working with the IceCube project to develop a cybersecurity plan tailored to the needs of the project that would protect and ensure the integrity of research data and IceCube resources. The engagement began in June of 2013 with the CTSC team traveling to the IceCube office in Madison to collect information about the IceCube environment in order to develop a system characterization document. The first step in the process was to conduct a risk assessment of the IceCube project to identify assets, risks, threats, and vulnerabilities. The assessment included a review of existing IceCube security policies and procedures. Members of both CTSC and IceCube participated in the assessment process to categorize and weight identified risks. This analysis was used to determine the best way resources can be applied to further strengthen IceCube's cyberinfrastructure.

As a result, CTSC proposed a cybersecurity improvement plan for IceCube's cyberinfrastructure, which is available publicly at http://trustedci.org/icecube/.

We were contacted in 2014 by the IceCube team about a security incident the project experienced in early May of 2014. The CTSC team scheduled several conference calls to review their response process and conduct a lessons learned activity. It was noted that a number of the suggestions in the IceCube cybersecurity improvement plan which they had not yet had opportunity to implement would have reduced the intrusion significantly. The incident also raised interest by IceCube in developing a formal IceCube incident response plan. The CTSC team pointed IceCube to the incident response template for the "Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects" to help accelerate this effort.

[21] http://icecube.wisc.edu/ - Funded by NSF GEO/PLR

7. 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. Towards this end, CTSC undertakes a set of Education, Outreach, and Training (EOT) activities.

7.1 Education

Our education activities focus on the undergraduate and graduate level. CTSC develops cybersecurity modules for undergraduate and graduate level courses that focus on important aspects of securing scientific CI. CTSC education modules are designed with two types of audience in mind: students with a background in computer security, but who may not be familiar with the security needs and requirements of scientific CI (target audience group 1); and students who are end users of CI, but who may not necessarily have a background in security (target audience group 2). Accordingly, the education modules developed will present topics in the context of scientific CI and can be incorporated into dedicated security courses (for target group 1) or into courses on other aspects of scientific computing (for target group 2).

Significant progress was made in year two on two educational modules covering characteristics and security needs of scientific CI: Federated Identity and Single Sign-on. These modules, targeted at cybersecurity students, in particular, those with a focus on delegation and single sign-on, were debuted in a senior level security course (CS 461/ECE 422 Computer Security I) at the University of Illinois this Fall 2013 and Spring 2014 . We will disseminate these modules freely via the CTSC website and are actively seeking additional adopters to provide feedback and improve the modules.

7.2 Outreach

CTSC undertakes outreach activities both to disseminate its work and to make NSF CI projects aware of its services. A highlight for the year was *International Science Grid This Week* featuring CTSC's work with LIGO and Internet2 on international federation in an online news story.[22]

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

[22] http://www.isgtw.org/spotlight/federated-trust-expands-internationally-edugain-declaration

cybersecurity news of interest to NSF CI projects (twitter.com/trustedci). A press release for the 2014 Cybersecurity Summit was also produced by CTSC.[23]

In addition to blog posts about CTSC activities, this year we initiated a series of blog posts on best practices in identity management, with the goal of providing guidance and how-to guides that are broadly applicable to NSF CI. The topics in the series were HTTPS Best Practices[24], Outsourcing Identity Management[25], and Self Service Password Reset.[26] Next year we plan a similar series of blog posts on software development security best practices.

Presentations made by CTSC included:

- Von Welch. Cybersecurity for Cyberinfrastructure and Science!. Presentation at 2014 HUBbub, September 2014. http://www.vonwelch.com/pubs/CTSC-HUBbub-Sep14
- Von Welch. Cybersecurity for NSF Science: What does that Mean?. Presentation at 2014 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure, August 2014. http://www.vonwelch.com/pubs/CTSC-Summit-Aug14
- Von Welch. CTSC: Trustworthy Scientific Cyberinfrastructure. Presentation to NSF CC-NIE Workshop, April 2014.http://www.vonwelch.com/pubs/CTSC-CCNIE-Apr14
- Von Welch. CTSC: Service Model and Experiences. Presentation to NSF SI2 PI Meeting, February 2014.http://www.vonwelch.com/pubs/CTSC-SI2-Feb14
- Von Welch. Scientific Data Security. Presentation to ASIS&T Bloomington Chapter, January 2014.http://www.vonwelch.com/pubs/ASIST-Jan14
- Craig Jackson, James Marsteller and Von Welch. 2013 NSF Cybersecurity Summit for Cyberinfrastructure and Large Facilities.Presentation to NSF Large Facilities Security Group (FacSec), December 2013. http://www.vonwelch.com/pubs/CTSC-FacSec-Dec13
- Von Welch. A view from the field of NSF cybersecurity challenges, goals, and opportunities.
- 2013 NSF Cybersecurity Summit for Cyberinfrastructure and Large Facilities, October 2013. http://www.vonwelch.com/pubs/CTSC-Summit-Oct13

In 2013, CTSC established the Trusted CI Forum (trustedci.groupsite.com) to support the ongoing community initially formed at the 2013 NSF Cybersecurity Summit. Usage of the forum by the community has been minimal. We have experimented with email lists to foster collaboration outside of the summit[27], but developing a strong ongoing community interaction remains a challenge.

---

[23] http://itnews.iu.edu/articles/2014/iu-project-receives-grant-to-host-nsf-cybersecurity-summits-in-2014-2015.php

[24] http://blog.trustedci.org/2014/04/https-best-practices.html

[25] http://blog.trustedci.org/2014/04/idm.html

[26] http://blog.trustedci.org/2014/07/r.html

[27] http://trustedci.org/ctsc-email-lists/

7.3 Training

Training for NSF CI professionals is a significant activity within CTSC and currently takes the form of lecture-style training materials delivered in person by CTSC staff. In CTSC's first year we developed a Risk-based Cybersecurity tutorial, capturing the process that CTSC utilized and refined in its engagements with LNO, CyberGIS, and IceCube. This tutorial was presented as a 4 hour long training session that educates NSF project PIs and management on the importance of cybersecurity from a science CI perspective, teaches them the basics of performing a risk assessment of their project, transitions from that into the design of a cybersecurity program, and outlines the steps to put such a program into operation. This training debuted at the 2013 NSF Cybersecurity Summit. Over the second year of the CTSC project, our engagement with the DKIST project significantly enhanced our expertise in this area and led to a much improved Risk-Based Cybersecurity tutorial, along with the guide on developing a cybersecurity program. This newly enhanced Risk-based Cybersecurity tutorial was presented at the 2014 NSF Cybersecurity Summit.

In year two we also added a 4 hour tutorial on Building an Incident Response Team which was presented for the first time at the 2014 NSF Cybersecurity Summit. (This brings the total number of tutorials CTSC has developed to three.) This new tutorial is also intended for CI professionals and walks them through four main areas: 1) an overview of the goals for incident response and a discussion of its key components; 2) the process of establishing an incident response capability, including an overview of risk assessment, related policy and procedure, detailed discussions about incident response-related security controls including an emphasis on monitoring systems and log management, and establishment of an incident response team; 3) a guide laying out a set of steps that walk the students through the incident response cycle; and finally 4) a set of four example investigations that utilized the steps outlined in step 3. The tutorial has the goal of preparing anyone for the steps it will take to develop and deploy an incident response program. While it is applicable to all incident team types it is primarily targeted for NSF CI teams that do not have a large team of incident responders or, more than likely, have a team that consists of members that have other full-time responsibilities on the project.

Also in year two, we updated our third tutorial, originally covering the topic of secure programming. The new material includes the basics of in-depth software vulnerability assessment, approach security from the viewpoint of an attacker, and new material on secure programming. The new secure programming material includes examples from scripting languages such as Ruby, Python, and Perl, and conventional languages such as Microsoft's C#. We also added coverage of topics such as serialization/deserialization, XML injections, and a section on coverage of mobile application coding errors.

To foster broader impact on a larger number of NSF CI project, CTSC developed a strategy to transform our training materials into YouTube videos. In the last year the Risk-based Cybersecurity tutorial was transformed into a series of YouTube videos that utilized our previously developed slide deck with the added benefit of a professional voice-over explaining them. This tutorial was broken into a series of 10 minute or less clips to make it easy for a student to casually cover all the material at their own pace. The videos are available at http://trustedci.org/onlinetraining/ and have resulted in over 700 total viewings.

We are now utilizing this same process to turn the Incident Response tutorial into a series of YouTube videos as well.

7.4 Student Training

CTSC supports the development of skilled cybersecurity professionals and researchers by directly engaging students in stimulating cybersecurity activities. In 2013 CTSC collaborated with Indiana University's successful Summer of Networking program[28] to provide a cybersecurity-focused internship for one student, Betsy Thomas, who researched and completed a theoretical design for an intrusion detection system for virtual organizations. Betsy and another Summer of Networking student, Epaphras Matsangaise, both continued to work with CTSC through the Spring of 2014 and the Fall of 2013, respectively, as hourly research assistants. Betsy Thomas has since gone on to work for Cigital, a software security company, and Epaphras for the Indiana University GlobalNoc.

Unfortunately, in 2014 the Summer of Networking program transitioned from an internship-based program to an academic program, which precluded CTSC mentoring students as it did in 2013. We plan to replace this activity with the direct mentoring of a student through an hourly research assistant position as we did with the students after the program in 2013.

8. 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 toward 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.

8.1 NSF Cybersecurity Summit

Since publishing CTSC's Year 1 Report, in line with CTSC's mission to provide cybersecurity leadership and education to the NSF CI community, the center has organized and executed the 2013 and 2014 NSF Cybersecurity Summits for Large Facilities and Cyberinfrastructure under supplemental awards. Spanning six years from 2004-2009, the NSF-funded annual Cybersecurity Summits served as a valuable part of the process of securing NSF-funded infrastructure and building a cybersecurity community by

[28] http://incntre.iu.edu/summer/

providing the opportunity to share best practices, educational opportunities from experts both within and outside of the community, and the opportunity to collaborate on solving common challenges.

The 2013 NSF Cybersecurity Summit developed around the theme, *Designing Cybersecurity Programs in Support of Science*, with an explicit focus on the challenges of supporting the community of practitioners and stakeholders who must secure scientific CI. The Summit spanned three days, September 30 through October 2, 2013. Despite falling on the first day of the U.S. federal government shutdown, preventing representatives from NSF from participating, sixty-nine (69) people attended the Summit, representing 24 NSF-funded projects and 30 organizations. The first day offered tutorials on four subjects (identity management, network security and monitoring, cybersecurity planning, and secure software development). Day 2 was in plenary, tackling the Summit's theme of Designing Cybersecurity Programs in Support of Science. On Day 3, the participants broke into working groups to tackle specific technical areas. The full 2013 summit report is available at http://hdl.handle.net/2022/17295.

Though the 2013 summit was very well-received, we felt the Summits could and should go further in supporting measurable progress on establishing reasonable community norms for the scope, metrics, resources, and processes for developing and implementing cybersecurity programs; providing pragmatic levels of information security; and supporting scientific discovery. Two findings of the 2013 Summit served as overarching drivers for the proposed 2014 and 2015 events:

> **Finding 5**. The community should consider the cybersecurity needs of and relationship between Large Facilities and smaller cyberinfrastructure projects, as well as how (and if) the summit can effectively address both.
>
> **Finding 6**. The community needs to develop a better understanding of the expectations for their cybersecurity programs and how to meet those expectations.

The 2014 Summit took place from Tuesday, August 26th through midday Thursday, August 28th, at the Westin Arlington Gateway near NSF, with the theme of *Large Facility Cybersecurity Challenges and Responses*. One hundred seventeen (117) people attended the event, including 22 NSF personnel and 3 student awardees (who responded to a call for participation and whose travel was covered by the supplemental award). On August 26th, we offered a full day of training in response to 2013's strong training attendance and overwhelmingly positive feedback. CTSC personnel participated as trainers in 3 of the 5 training sessions, with the other two sessions being offered by members of the broader community. The second and third days were in plenary, with keynotes, panels, and speakers focused on both the key cybersecurity challenges facing Large Facilities and the most effective responses to those challenges. To elicit an increasing degree of community participation, much of the agenda was based on responses to a call for participation issued prior to the Summit, and August 27th's lunch included table topic discussions of a variety of specific information security issues. Adding to the breadth of perspective and discussion of risk-based approaches to information security, the program committee recruited two esteemed keynote speakers:

Dr. Phyllis Schneck, Deputy Under Secretary for Cybersecurity for the National Protection and Programs Directorate within the Department of Homeland Security (DHS). Dr. Schneck is the chief cybersecurity official for DHS and supports its mission of strengthening the security and resilience of the nation's critical infrastructure.

Matthew Rosenquist, Cybersecurity Strategist, Intel. Mr. Rosenquist specializes in security strategy, measuring value, and developing cost effective capabilities which deliver the optimal level of security.[29]

As of the time of the writing this report, the 2014 Summit report is in an early draft phase and will be published by the end of calendar year 2014. Information regarding the event (e.g., agenda, biographies, presentations) is most readily accessible at http://trustedci.org/2014summit/. The report will contain the full results from surveys completed by attendees. Initial results of attendee surveys (and additional anecdotal reports) indicate the Summit was very well received, perhaps with even greater enthusiasm than in 2013. CTSC has secured funding and initiated plans for a 2015 Summit, envisioning the Summit as an ongoing annual event.

8.2 CTSC Cybersecurity Program

CTSC itself is an NSF CI project and hence in year one followed its own guidance and developed its own cybersecurity program. CTSC has made its program publicly available[30], along with supporting documentation, in order to both provide an example to the community and help establish the trust of potential engagees that their information will be appropriately protected.

In year two, CTSC reviewed this cybersecurity program and is in process of making minor updates to keep it up-to-date with changes in CTSC and the threat landscape. This program will be finalized at CTSC's internal all-hands meeting and published in October of 2014.

8.3 CTSC Whitepapers and Technical Reports

CTSC's leadership efforts include the publication of papers providing guidance to the community and stating opinions of direction to unify community approach. CTSC's contribution in project year two were as follows:

---

[29] See Rosenquist's blog post about the talk and his impressions of our community here: https://communities.intel.com/community/itpeernetwork/blog/2014/09/23/strategic-leadership-for-managing-evolving-cybersecurity-risks

[30] http://trustedci.org/cybersecurity-program/

- "Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects." This guide along with supporting templates and training materials is available at http://trustedci.org/guide.
- "Securing Commodity IT in Scientific CI Projects: Baseline Controls and Best Practices." http://trustedci.org/guide/docs/commodityIT

8.4 Collaboration with NSF-funded Bro Center of Expertise

In October of 2013, NSF funded the Bro Center of Expertise (https://www.bro.org/nsf/) to provide expertise from the Bro team to NSF projects. Given the alignment between in the missions of CTSC and the Bro Center, collaboration was natural and took the form of:

- Coordinated training with the Bro team providing training at both the 2013 and 2014 NSF Cybersecurity Summits for Large Facilities and Cyberinfrastructure.
- Collaboration on CTSC's Peer Review between CC-NIE projects described previously in this report.
- A proposal to XSEDE'14 for a BoF on "National Cybersecurity Resources for Scientific Research."
- Monthly phone calls to coordinate and explore opportunities for collaboration.

8.5 Interagency, Higher Education, and International Collaborations

Fostering interoperability between NSF CI and the global research computing ecosystem is a key goal in CTSC efforts. To that end, in addition to the previously described international identity federation efforts with LIGO and the InCommon EduGain working group, CTSC is maintaining strong ties with DOE, through key invitations to the NSF Cybersecurity Summit, and DHS activities, through Welch and Basney's role as co-PIs in the DHS Software Assurance Marketplace. We maintain good ties with the Internet2 and the Higher Ed community through Basney's participation on the InCommon Technical Advisory Committee. Additionally, our advisory committee, discussed in the next section, provides us with further ties to these communities.

CTSC has also worked with ESNet to foster the dissemination of their work on security for science DMZs[31] to the NSF community. The projects collaborated to submit a BoF proposal to SC14 and a panel to Internet2 Tech Exchange. The BoF proposal was not accepted but the panel proposal was and will take place in October 2014.[32]

---

[31] http://fasterdata.es.net/science-dmz/science-dmz-security/

[32] http://meetings.internet2.edu/2014-technology-exchange/detail/10003410/

CTSC also collaborated with SWAMP, DETER, the Bro Center of Expertise, and the XSEDE Campus Champions program to submit a BoF proposal to XSEDE'14 on "National Cybersecurity Resources for Scientific Research." This proposal was unfortunately not accepted.

CTSC further has a connection to the National Security Higher Education Advisory Board (NSHEAB) through the Cybersecurity Subcommittee, of which co-PI Butler is a member. This advisory board is hosted by the FBI, NHS, and CIA, and includes eight members of higher education that work with the agencies to discuss and develop methods for a broader sharing of actionable cybersecurity intelligence to the higher education community.

9. 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[33]).

The CTSC advisory committee members are:

- Tom Barton - senior director for architecture, integration and chief information security officer at the University of Chicago.
- Neil Chue Hong - 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 - senior project manager for research in cybersecurity at the Pacific Northwest National Lab (PNNL) in Richland, Washington.
- Nancy Wilkins-Diehr - director of Consulting, Training, and Documentation at the San Diego Supercomputing Center. Nancy 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/.

[33] http://supercomputing.org/

10. Lessons Learned

CTSC continues to evolve its lessons learned, as first reported in its year one report. The lessons follow (order is not meaningful).

10.1 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 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.

10.2 Engagements Require Flexibility and Innovation

Having completed more than a 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

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.

10.3 The Summit is Critical to Community Building and Outreach

CTSC has now hosted two 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.

10.4 Venues for Delivering Training are Scarce

There aren't many venues currently 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 to deliver 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.

10.5 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.

10.6 Leveraging Campuses is Possible to a Degree

As we described previously, 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.

10.7 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.

10.8 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 two 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 bringing broader information security best practices to bear.

11. Year 3 Plans

In this section we describe CTSC's plans for project year 3 (Oct 1, 2014 - Sep 30, 2015).

11.1 Engagements

CTSC will continue to spend the majority of its effort on engagements with NSF CI projects to address their cybersecurity challenges. In our proposal and subsequent revised statement of work, we indicated we would undertake four engagements in year three, and we expect to initiate at least that many. Projects with which we have already had discussions about a potential year three engagement include: LSST, Gemini, NEON, UCAR, and the University of Pittsburgh CC-NIE.

11.2 Engagement Follow-ups

It is critical to CTSC to ensure that our engagements are having impact to the collaborating projects. We will follow up with each of the projects we engaged with in years one and two to solicit feedback on how our engagement impacted the project once some time has passed.

11.3 Education, Outreach and Training

In CTSC project year three, we will continue to transform our training materials into an electronic delivery form via YouTube with the goal of making these tutorials available for on-demand access by the community. Specifically we will transform the Incident Response tutorial into a series of YouTube videos in the coming year to augment our existing videos.[34]

We will further enhance our collaboration with the NSF-funded Bro Center (PIs: Sommer and Slagell), focused on network security and monitoring training. The collaboration between these two groups will include sharing material and coordinating venues as well as a closer coordination on the development of training materials. We currently have an open job posted for a training coordinator that will be jointly funded by CTSC and Bro. We note that the two teams have already collaborated on training at the last two NSF Cybersecurity Summits.

CTSC will also develop new training materials; currently we are working on the development of a Password Best Practice Guide which we plan to turn into a tutorial and YouTube videos. Additional

[34] http://trustedci.org/onlinetraining/

training topics will be investigated in year 3 and we anticipate at least one more additional topic being identified.

Our team member who led Education activities accepted a position at another university and we currently have no lead on this work. Our biggest hurdle to overcome however is the lack of an Education lead but we will work with the University of Illinois Computer Science department to identify a potential home for the materials already developed and seek out a partner to take on the education lead.

Education activities in year 3 will focus on lessons learned and feedback obtained from the use of modules in the senior level computer security course at the University of Illinois, which will inform any development of these education modules in year 3. We will actively work to engage faculty at University of Illinois and other universities to make them aware of our existing modules.

Outreach activities will continue to focus on producing best practices and other contributions aimed at guiding the community. We will produce white papers with guidance on password management and getting started with software assurance.

The University of Wisconsin team will concentrate on two areas in the coming year. First we will cover new topics in our tutorials. The first topic will focus on using static analysis tools for finding program weaknesses, including background on the underlying technology used by these tools and their capabilities and limitations. The second new topic will involve examples from mobile applications. In addition, we will introduce practical, hands on materials to go along with their tutorials on vulnerability assessment and secure programming. These materials will include the software infrastructure (delivered via virtual machine) and instructional presentations and documents to direct the students.

11.4 2015 NSF Cybersecurity Summit

We have already obtained funding via a supplement for the 2015 NSF Cybersecurity Summit. We will push forward with our vision of the NSF Cybersecurity Summit as the nexus for a NSF CI Community to collaborate on cybersecurity. We are still evaluating feedback from the 2014 Summit, and a specific technical focus for the 2015 Summit will be determined based on that feedback and input from the community.

12. Conclusion

This report covers CTSC's successful second year, during which time CTSC engaged seven NSF CI projects directly (bringing its total over the first two years to 13), re-invigorated the NSF CI cybersecurity community by organizing the 2013 and 2014 NSF Cybersecurity Summits for Large Facilities and Cyberinfrastructure, provided the community with a guide and templates for developing a cybersecurity program, and provided training in secure coding, incident response and developing a cybersecurity program. CTSC impact on the NSF CI community has been impressive, with nearly 150 individuals, representing over 70 projects, attending one or both of the Summits, over 130 CI professionals representing 30 projects attending CTSC-led training. Those numbers include a significant impact on NSF Large Facilities, who comprised 4 CTSC engagees, 14 of the projects who have attended one or both Summits, and 9 of the projects benefitting from CTSC training. CTSC's outreach also had significant accomplishments including an article in *International Science Grid This Week* on CTSC's work with LIGO and a NSF solicitation mentioning the CTSC-organized Summit.

References

- [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]
- [Pegasus] Ewa Deelman, Gurmeet Singh, Mei-Hui Su, James Blythe, Yolanda Gil, Carl Kesselman, Gaurang Mehta, Karan Vahi, G. Bruce Berriman, John Good, Anastasia Laity, Joseph C. Jacob, Daniel S. Katz. Pegasus: a Framework for Mapping Complex Scientific Workflows onto Distributed Systems - Scientific Programming Journal, Vol 13(3), 2005, Pages 219-237.
- [Pegasus-CTSC] R.W. Heiland, S. Koranda, V.S. Welch, "Pegasus-CTSC Engagement Final Report," Center for Trustworthy Scientific Cyberinfrastructure, trustedci.org, May 2013. Available: http://hdl.handle.net/2022/15562
- [LIGO-CTSC] Basney, J., Koranda, S. Center for Trustworthy Scientific Cyberinfrastructure Engagement Plan: Final Report for LIGO Engagement. July, 2013. http://hdl.handle.net/2022/16689
- [LIGO-Three] Basney, J., Koranda, S. A Study of Three Approaches to International Identity Federation for the LIGO Project. July, 2013. http://hdl.handle.net/2022/16760
- [LIGO-eduGAIN] Basney, Jim; Koranda, Scott. InCommon Membership in eduGAIN: the LIGO Perspective. May, 2013. http://hdl.handle.net/2022/16690
- [Wilkins-Diehr] Wilkins-Diehr, N. A History of the TeraGrid Science Gateway Program: A Personal View. Proceedings of the 2011 ACM Workshop on Gateway Computing Environments (GCE '11). Nov 2011. doi:10.1145/2110486.2110488
- [Saltzer1975] Saltzer and Schroeder. The Protection of Information in Computer Systems, 1975. http://web.mit.edu/saltzer/www/publications/protection/
- [Saltzer2009] Saltzer and Kaashoek. Principles of Computer Design, 2009. http://books.google.com/books?id=I-NOcVMGWSUC
- [Smith2012] R.E. Smith, A Contemporary Look at Saltzer and Schroeder's 1975 Design Principles, 2012. http://cryptosmith.com/node/365