
# Year 1 Report

## Center for Trustworthy Scientific Cyberinfrastructure

NSF ACI Grant # 1234408
Covering Project Year 1
October 1, 2012 – September 30, 2013

*For Public Distribution*

CTSC Team

Jim Basney[3] (co-PI), Rakesh Bobba[3], Randy Butler[3] (co-PI), Patrick Duda[3], Terry Fleury[3], Randy Heiland[2], Elisa Heyman[4], Craig Jackson[2], Scott Koranda[5] (co-PI), Jim Marsteller[1] (co-PI), Prof. Barton Miller[4] (Senior Personnel), 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) 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



This work is available in electronic form at:
http://trustedci.org/reports
and
http://hdl.handle.net/2022/17205

# 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 readily available cybersecurity expertise and services, as well as leadership in advancing the state of practice and coordination across a broad range of NSF scientific CI projects via a series of engagements with NSF CI projects and a broader ongoing education, outreach and training effort.

The vision of CTSC is an NSF CI community in which 1) each project knows where it fits in a coherent cybersecurity ecosystem and can assess its own needs; 2) each project has access to the tools and needed help to enact a basic cybersecurity program and tackle the project's advanced challenges; 3) sharing of experiences and collaboration between projects is the norm; and 4) cybersecurity is greatly benefited by leveraging services, universities, I2, and broader community best practices.

Towards this vision, CTSC is organized by three thrusts: 1) **Engagements** with specific communities to address their individual challenges; 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 coherent, interoperable cybersecurity community and ecosystem.

This report covers CTSC's successful first year, in which it initiated seven engagements, completing three (LTER Network Office, LIGO, Pegasus), is in the process of finalizing three more (DataONE, IceCube, CyberGIS) and initiating a seventh (Globus Online). Accomplishments include 1) developing a process for developing NSF CI Cybersecurity programs that incorporates well-known best practices and tackles NSF CI challenges of residing in a complicated, multi-institution ecosystem with unique science instruments and data; 2) re-starting and organizing the NSF Cybersecurity Summit along with an online Trusted CI Forum to foster an ongoing NSF community focused on NSF CI cybersecurity; and 3) delivering seven training sessions by leveraging prior training materials from the University of Wisconsin team and creating two new tutorials. Educational activities include 1) creating a new education module on cybersecurity for CI that is being utilized in a class at the University of Illinois this Fall; 2) mentoring of a student in Indiana University's Summer of Networking program; 3) and the ongoing membership of two graduate students in the CTSC team as research assistants. Our broader impacts include the publication of engagement products and three other papers to define community best practices.

Year two plans are described that continue the emphasis on these three thrusts and building the community working on cybersecurity with the Trusted CI Forum and a vision for continued CI and Large Facility Cybersecurity Summits.

# Table of Contents

# 1 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). CTSC is providing readily available cybersecurity expertise and services, as well as leadership and coordination across a broad range of NSF scientific CI projects via a series of engagements with NSF CI projects and a broader ongoing education, outreach and training effort.

As NSF pushes towards its vision of "a comprehensive, integrated, sustainable, and secure CI," cybersecurity plays a key role. However, two recent Scientific Software Security Innovation Institute workshops [1], which included representatives of 35 major NSF-funded CI projects, determined that the NSF CI community faces strong challenges in obtaining access to cybersecurity expertise. Projects are forced to divert their resources to develop that expertise, address risks haphazardly, unknowingly reinvent basic cybersecurity solutions, and struggle with interoperability.

Contributing to the need for expertise is the fact cybersecurity is not a challenge to be solved by a single technology solution. Every project has its own culture, risk tolerance, legacy technologies, collaboration patterns, and timelines, making a technological "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. It leads 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 1) each project knows where it fits in a coherent cybersecurity ecosystem and can assess its own needs; 2) each project has access to the tools and needed help to enact a basic cybersecurity program and tackle the project's advanced challenges; 3) sharing of experiences and collaboration between projects is the norm; and 4) cybersecurity is greatly benefited by leveraging services, universities, I2, and broader community best practices.

Towards this vision, CTSC is organized by three thrusts: 1) **Engagements** with specific communities to address their individual challenges; 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 coherent, interoperable cybersecurity community and ecosystem.

# 2 Engagements

One of CTSC's three thrusts is an ongoing set of engagements with NSF-funded scientific CI projects to solve cybersecurity challenges faced by those projects. During the first year, CTSC completed engagements with the LTER Network Office, the LIGO Scientific Collaboration and Pegasus; engagements with CyberGIS, DataONE, and IceCube are wrapping up at the end of the year; and a new engagement with Globus Online is underway. As CTSC enters year two we are already in discussion with other projects (SEAD, Open Science Data Cloud) as potential engagements and plan on an open call for engagements as described in our Year 2 Plans.

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 the three completed engagements, we solicited and included a statement from the project regarding the engagement. We will solicit feedback from the other year one engagements in year two.

In addition to these larger engagements, CTSC has recognized a need for shorter, informal interactions with projects that may turn into longer engagements or may satisfy a project's needs in themselves. In our first year, CTSC staff reviewed a technical plan for certificate renewal for the Open Science Grid and provided the SEAD project with basic guidance for identity management. As we discuss in our Year 2 plans, we will be more explicit in offering this type of assistance to the NSF community.

CTSC declined one engagement in its first year, an XSEDE science gateway project which we determined would be best served by the XSEDE project directly.

## 2.1 LTER Network Office

The Long Term Ecological Research Network (LNO)[1] 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.

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

PASTA is a developing model for dynamically harvesting and archiving site-based data and metadata of the LNO for use in generating synthetically derived data products. These derived data products are then accessed through multiple user and machine interfaces. All derived data are described by a rich and structured Ecological Metadata Language (EML) document, which emphasizes the product processing history and its origin – the product "provenance".

PASTA serves the ecological community with access to the data and analysis tools produced by the LTER sites and projects. It provides a portal based entry to search, analyze, contribute data, and more. A key focus of the engagement was to assess the PASTA identity and access management system that registers users, authenticates them, and applies authorizations to data, users, and services.

The result of our the team effort between LNO and CTSC was to document and prioritize the LNO PASTA risks and then design a cybersecurity plan that addressed the identified risks with a combination of security best practices and additional controls for specific risks. The risk assessment and cybersecurity plan were delivered to LNO, who have been actively implementing the plan to protect the PASTA data repository.

Mark Servilla, Lead Scientist at LNO, provided the following statement:

> *The Center for Trustworthy Scientific Cyberinfrastructure (CTSC) convened its first cyber-security review and assessment of the Long Term Ecological Research (LTER) Network Office and the Provenance Aware Synthesis Tracking Architecture (PASTA) in February 2013. The engagement started with a 3-day meeting which was prefaced by an extensive analysis of LTER Network policies, procedures, and architecture. The CTSC team was thorough in their analysis and professional in their demeanor. Two significant artifacts were produced: (1) a cyber-security assessment of existing practices and architecture and (2) a forward-looking cyber-security plan for the LTER Network Office and PASTA.*
>
> *The cyber-security assessment provided detailed review of existing LTER Network Office practices and architecture and provided a necessary baseline from which to gage change and improvement. Specifically, the assessment identified strengths and weaknesses of current cyber-security practices followed by the LTER Network Office and of the nascent PASTA framework of the Network Information System. This latter aspect of the assessment occurred a fundamentally critical point in system design such that issues could easily be mitigated prior to the full production release of PASTA. The assessment also prioritized cyber-security countermeasures that became the foundation of LTER Network Office Cyber-security Plan.*
>
> *The LTER Network Cyber-security Plan is a forward looking approach to increasing cyber-security for LTER Network assets (data and infrastructure). The*

*plan is structured such that highest risk elements of LTER Network assets are protected early on in the implementation strategy, while lower risk elements or those already protected reasonably well are addressed later. The CTSC team, in developing the plan, also provided reference to public and commercial software resources and infrastructure that may be utilized by the LTER Network Office in building cyber-security defenses.*

*In summary, the CTSC review and assessment provided crucial insight into existing cyber-security practices and architecture of the LTER Network Office and the PASTA framework. This effort set a baseline reference from which meaningful change can be measured and provided a concrete and specific cyber-security plan for LTER Network office personnel to implement.*

## 2.2 DataONE

DataONE (Data Observation Network for Earth)[2] is a federated data network built to improve access to Earth science data, and to support science by: (1) engaging the relevant science, data, and policy communities; (2) facilitating easy, secure, and persistent storage of data; and (3) disseminating integrated and user-friendly tools for data discovery, analysis, visualization, and decision-making.

DataONE has invested significant effort into the development of an identity management (IdM) system that supports federated identities from a wide variety of identity providers and includes mechanisms and procedures to support access management. The DataONE identity management system forms the trust fabric by which DataONE Member Nodes, Coordinating Nodes and users interact, and hence is critical to DataONE's long-term success. CTSC and DataONE collaborated on a design-level review of the DataONE IdM system implementation with the following goals:

- Identify the specific software components to be reviewed.
- Identify (or assist in creating) documentation of those components sufficient to review them.
- Perform and document an assessment of those components that is of use to DataONE.
- Assess potential vulnerabilities, scalability, interoperability and supportability

Aspects of DataONE's IdM system that were examined included Member Nodes, Coordinating Nodes, CILogon, certificate management, identity mapping and the Identity API and Authorization API. Other off-the-shelf components such as LDAP were not the focus of the review. Furthermore, the DataONE project internal IDM system for project collaboration was out of scope.

[2] http://www.dataone.org/ - funded by NSF ITR/DATANET

The review process was conducted at a two day face-to-face meeting between the CTSC and DataONE teams. This meeting was held in an informal ad-hoc style. Prior to the face-to-face meeting, the CTSC team reviewed documents identified by DataONE as being valuable to understanding the IdM system.

CTSC is preparing a report documenting the review findings. This report includes a system characterization describing the DataONE IdM system and CTSC's review of DataONE's documentation of their IdM system. The report is substantially complete at this time, CTSC and DataONE have already discussed the findings, and CTSC is finalizing the report by providing extra guidance to DataONE on certain topics per their request.

With the growth of federated identity and projects (e.g., Globus Online, CILogon, iRods) supporting multiple forms of authentication, systems such as DataONE's IdM system are becoming more common. Identifying and documenting best practices and lessons learned for such systems will have broad impact across current and future systems. As a recoverable for future engagements, CTSC plans to create a document describing a general set of principles for similar identity management systems and process for assessing those systems.

## 2.3 Pegasus

Pegasus[3] is a workflow management system (WMS) for scientific workflows [2]. Quoting from the Pegasus website: "Pegasus bridges the scientific domain and the execution environment by automatically mapping high-level workflow descriptions onto distributed resources. It automatically locates the necessary input data and computational resources necessary for workflow execution. Pegasus enables scientists to construct workflows in abstract terms without worrying about the details of the underlying execution environment or the particulars of the low-level specifications required by the middleware (Condor, Globus, or Amazon EC2). Pegasus also bridges the current cyberinfrastructure by effectively coordinating multiple distributed resources."

Pegasus workflows typically operate across distributed resources and sometimes need to stage data files between compute resources to or from storage resources. When such staging requires secure shell (SSH), Pegasus' current practice is to send a private key with the workflow to perform a secure copy. The goal of this engagement was to examine this practice and recommend any possible improvements from the perspective of cybersecurity.

The report produced by our engagement [3], develops a set of security criteria by which to judge different options that could be implemented by the Pegasus project. Based on those criteria, we provides three recommendations to the Pegasus team to improve current practice: (1) If system administrators are willing, have them deploy a mechanism that supports security delegation, such as Kerberos or GSI; (2) provide assistance to users in using SSH's ability to impose restrictions in the *authorized_keys* file to limit the privileges of SSH keys used for

[3] http://pegasus.isi.edu/ - funded by NSF SI2, suporting many projects: http://pegasus.isi.edu/applications

workflows; and (3) utilize ssh-agent to minimize exposure of SSH credentials in the workflow by avoiding writing those credentials to the filesystem. Our report also describes alternatives we considered, but did not recommend and considers the relevant use case of using Pegasus with Amazon S3.

Pegasus' challenge is a general one, potentially faced by any workflow system. Hence, our report was made publicly available to benefit the broader community.

Ewa Deelman, Pegasus PI, provided the following statement:

> *Our engagement with CTSC focused on the problem of how to avoid the storage of SSH credentials on the local filesystem of the worker nodes for the duration of job execution. The CTSC team came up with a set of recommendations some of which we plan to incorporate in Pegasus in the near future. During this exercise, the two teams also explored various alternatives that initially looked promising and feasible, but later had to be discounted because of potential security holes or increased complexity of the system.*
>
> *Overall, we would characterize the engagement as a success, as it has helped us identify and formalize various solutions. The associated engagement report will serve an blueprint on how to tackle this problem and we feel that it's applicability is not limited only to Pegasus but to other systems that support distributed execution of jobs.*

## 2.4 LIGO

The Laser Interferometer Gravitational-Wave Observatory (LIGO) Scientific Collaboration[4] 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.

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. The objective was to

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

characterize each approach and determine if all three would be needed to support LIGO's interfederation goals.

The three efforts were:

1. Establishing a point-to-point federation between LIGO service providers and an identity provider able to authenticate and assert attributes for members of the KAGRA[5] project in Japan.
2. LIGO joining the Italian IDEM SAML federation operated by GARR[6], the Italian National Research and Education Network (NREN), in order to support federation between LIGO services and users in the Virgo[7] project, a French and Italian project to detect gravitational waves.
3. To leverage LIGO's existing investment in InCommon, establishing a bilateral federation between InCommon in the US and the UK Access Management Federation for Education and Research (UK Federation). The UK federation was chosen because of the large number of existing LIGO collaborators in the UK and because InCommon and the UK already had begun some interfederation work.

Of the three efforts, the point-to-point federation with a KAGRA identity provider was underway already when the CTSC and LIGO engagement began, but the effort was intensified and focused by CTSC staff. CTSC and LIGO staff initiated the other two efforts directly as part of the CTSC and LIGO engagement.

The point-to-point approach with the KAGRA identity provider demonstrated that point-to-point federations continue to be useful even as larger and more comprehensive international interfederation agreements are pursued. Point-to-point federations are simply easier and more efficient for focused efforts aimed at enabling collaboration for specific groups of researchers.

The second effort, with LIGO attempting to join IDEM, stalled with the legal department at the California Institute of Technology (Caltech). The stall reinforces that barriers remain high for virtual organizations and projects seeking to join national identity federations, where the traditional process is tailored to higher education institutions, and legal obligations and liability play a significant role in negotiating membership.

The third effort leveraged LIGO's existing investment in InCommon. The CTSC/LIGO staff chartered the InCommon Technical Advisory Committee (TAC) Interfederation Subcommittee.[8] The committee included the CTSC/LIGO engagement staff, InCommon Operations staff, UK Federation staff, and interested members of the broader community. To investigate and support the LIGO use case, the committee pursued an exchange of select SAML metadata between InCommon and the UK Federation. The effort built upon work already underway in the

[5] http://gwcenter.icrr.u-tokyo.ac.jp/en/
[6] https://www.idem.garr.it/en
[7] http://www.ego-gw.it/virgodescription/pag_4.html
[8] https://spaces.internet2.edu/x/DAMlAg

UK to support interfederation trials.[9] The committee focused on the specific use case of federating a Cardiff University identity provider with the main LIGO wiki, with the goal of allowing both LIGO collaboration members at Cardiff and their colleagues with research interests in astronomy and astrophysics to reach the LIGO wiki using their Cardiff identities. This goal was achieved: LIGO collaboration members at Cardiff have accessed wiki.ligo.org using their Cardiff identities. LIGO did not join the UK federation nor directly insert metadata into the UK federation but instead leveraged its membership in InCommon to effect the metadata exchange to meet this goal.

A secondary goal of the CTSC-LIGO engagement was to assist LIGO by improving IdM collaborations with LIGO-India. This involved the development of federation use cases in support of the LIGO science mission, to be used as a driver for the continued development of a viable SAML identity federation in India, as well as assisting LIGO with training of LIGO-India staff on issues of federated identity management. In February 2013 Scott Koranda from CTSC and LIGO and Stuart Anderson from LIGO traveled to The Inter-University Centre for Astronomy and Astrophysics (IUCAA) in Pune, India for a three day meeting where they presented an introduction to and training on identity management for scientific organizations in general and for LIGO specifically, with an emphasis on SAML identity federations and interfederation. The training material developed by CTSC/LIGO for the visit is available online[10] and may be repurposed for use with other scientific organizations.

In conclusion, 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 joint CTSC-LIGO effort demonstrated prototype interoperability between a LIGO service and a UK identity provider, and as an additional outcome the effort also brought InCommon closer to joining the international eduGAIN[11] interfederation project. The effort also brought LIGO closer to interoperability with federations in India and Italy. Continued effort on interfederation by LIGO and InCommon is expected.

The CTSC-LIGO engagement produced three technical reports:

- Final Report for LIGO Engagement [4]
- A Study of Three Approaches to International Identity Federation for LIGO [5]
- InCommon Membership in eduGAIN: the LIGO Perspective [6]

Additionally, the identity management training has been generalized and will be delivered at the subsequently described Cybersecurity Summit.

[9] http://www.ukfederation.org.uk/content/Documents/InterfederationTrialFAQ
[10] https://dcc.ligo.org/LIGO-G1300690/public
[11] http://www.geant.net/service/eduGAIN/Pages/home.aspx

Warren Anderson, project manager for the LIGO Identity and Access Management project, provided the following statement:

> *LIGO is an international astronomy effort funded by the NSF to detect gravitational waves, a phenomenon predicted by Einstein in 1916 but not yet experimentally verified. The LIGO Scientific Collaboration is a body composed of over 1000 scientists from 20 countries on five continents. Furthermore, LIGO is part of a broader international gravitational wave community, with partner experiments in Germany, Italy and Japan. Finally, 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. In short, LIGO is part of a global astronomical network.*
>
> *A key tool of any scientific collaboration is an easily accessed and managed collaborative space. Over the past five years, LIGO has worked toward and Identity and Access Management solution involving industry standard tools such as Kerberos and OpenLDAP augmented by Internet2 middleware (Grouper and Shibboleth) and similar enabling technologies (e.g. CILogon) to provide a framework for building a collaborative space within LIGO. This does not in itself, however, address the problem of collaboration with the larger gravitational-wave astronomy community or our multi-messenger partners.*
>
> *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. For instance, LIGO still does not have in place identity federation with a number of our important scientific partners, including VIRGO, an Italian-French gravitational wave project who is currently our closest collaborator. By beginning the enrollment process for LIGO in IDEM, CTSC has helped clearly identify one of the key limiting factors in current processes for scientific collaborations like LIGO. Unlike many entities that need federated identity, LIGO is a loose affiliation of groups from various research institutions and has no legal standing on its own. Therefore, any contractual obligations LIGO wishes to engage in require the backing of one or more legal entities involved - usually one of the universities which administer the LIGO operating grants. In the case of IDEM, the campus which was asked to enter into the contractual agreement with the Italian IDEM SAML federation was the CalTech Institute of Technology (CIT). However, CIT legal is loathe to enter into contracts involving people and resources which they are not directly responsible for, which is the case for much of LIGO. This points clearly to the need for inter-federation at a higher level that provides an umbrella for the needs of scientific collaborations such as LIGO.*

*As an example, CTSC has enabled us to test internationally federated identity within LIGO through the engagement between InCommon and the UK Access Management Federation for Education and Research. However, this is only the beginning of what LIGO needs. With the upgraded sensitivity of second generation of LIGO, expected to come online within the next few years, first detection of gravitational waves (and subsequent detections) are expected to happen at timescales of months to weeks after observation begins. The pressure for coordinated observations and collaboration can reasonably be expected to exponentiate at this time. 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. Having international identity federation agreements and infrastructure in place at that time will greatly ease this pressure. LIGO sincerely hopes that CTSC will play a lead role in enabling such agreements and infrastructure going forward.*

## 2.5 IceCube

The IceCube South Pole Neutrino Observatory[12] 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 to protect and ensure the integrity of research data and IceCube resources. The engagement began in June 2013 with the CTSC team traveling to the IceCube office in Madison to collect information about the IceCube environment to develop a system characterization document. Once we had the system characterization completed the team began working on the risk assessment. The IceCube team has been very interactive during the engagement, reviewing the supporting documents in a shared repository. The assessment phase included reviewing the existing security policies IceCube has developed. At the time of this report, the risk assessment is nearly complete and cybersecurity plan development has begun. In addition to the planned engagement deliverables, CTSC will be providing the IceCube project with a Security Best Practices Guide for Commodity Information

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

Technology. This guide will also be made publicly available on the CTSC website as a resource for the CI community. The engagement is scheduled to be completed in November 2013.

## 2.6 CyberGIS

The CyberGIS project[13] seeks to use CI to allow researchers to interact with large data sets and complex analysis software, something not commonly found with conventional Geographic Information System (GIS) software approaches. While the CyberGIS project consists of many activities, the CyberGIS-CTSC engagement chose to focus effort on the CyberGIS Gateways.

The CyberGIS Gateways are web-based portal which allows end-users to run various GIS-based software packages on datasets. End-users can upload and manage their own (potentially private) datasets, or access publicly available datasets such as those provided by the U.S. Geological Survey (USGS). There are two CyberGIS Gateways available to users. The first has a larger list of available "apps" with an older interface, while the second has a small list of "apps" with a new user interface design. It is anticipated that the interface of the second Gateway will eventually supplant the main Gateway interface.

CyberGIS implements its own identity access management system, with each Gateway having its own user database. User access to the Gateways is granted with a simple username / password login page. While currently the majority of users are US-based researchers and students, with backgrounds in GIS, disaster management, and disease modeling, the Gateways are designed for a broad spectrum of users who may not have extensive experience in GIS. Thus, the interface is meant to be as simple as possible while allowing access to powerful GIS software.

CTSC met with CyberGIS personnel to perform a risk assessment of the CyberGIS Gateway system architecture. CyberGIS developers also sought solutions to specific questions regarding their code development and server configuration. CTSC performed and documented a detailed risk assessment outlining several vulnerabilities and possible controls for these vulnerabilities. The risk assessment was used as the basis for a cybersecurity plan. This plan categorized issues as problems with documentation, architecture, or operations. The plan then recommended tasks to address the issues sorted into short- (could be done in the order of weeks), medium- (would take on the order of months), and longer-term tasks. CTSC also addressed the specific questions from CyberGIS developers by creating a list of Suggested Best Practices consisting of detailed implementation solutions. CTSC is currently in discussion with the CyberGIS project regarding making the Engagement results public.

[13] http://cybergis.org/ - Funded by NSF SI2 in conjunction with NSF SBE/GSS

## 2.7 Globus Online

In September of 2013, CTSC began an engagement with the Globus Online (GO)[14] team at the Argonne National Laboratory and University of Chicago. The GO flagship service provides a "...fast, reliable file transfer service that makes it easy for any user to move any data anywhere. Recommended by HPC centers and user communities of all kinds, Globus Online automates the time-consuming and error-prone activity of managing file transfers, so users can stay focused on what's most important: their research." Recently the GO team added functionality to support sharing, i.e."big data sharing and transfer with dropbox like simplicity"[15]. GO is used by a number of NSF and other projects[16], making it an important CI component in terms of cybersecurity for the NSF CI ecosystem.

The primary focus of the CTSC/GO engagement is 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 GO team is collecting and preparing design and architecture documentation to share with CTSC staff and aid in the formal construction of the engagement plan.

# 3 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.

## 3.1 Training

Providing cybersecurity training to professionals in NSF CI community is a significant activity within CTSC and currently takes the form of lecture-style training materials delivered in person by CTSC staff. During CTSC's first year, primarily leveraging the prior work of the University of Wisconsin team, tutorials have been given at major venues, including XSEDE 2013, ESSOS 2013 (International Symposium on Engineering Secure Software and Systems), Condor Week 2013, and Supercomputing 2012. Additionally, special training sessions were delivered to the DHS-funded Software Assurance Marketplace (SWAMP)[17] implementation team and the LIGO-India staff. CTSC will also be presenting three training sessions at the upcoming NSF Cybersecurity Summit. Under other funding, the University of Wisconsin team leveraged the CTSC-developed

[14] https://www.globusonline.org/ - Funded by NSF SI2
[15] Private communication with the GO team.
[16] https://www.globusonline.org/stories/
[17] http://continuousassurance.org/

materials in presenting training sessions at Infosys (India's second largest IT company) and at the University of Chile.

CTSC development of new training materials over the first year have been focused on: (1) extending previous work at the University of Wisconsin on secure coding and vulnerability assessment; (2) the development of a tutorial on identity management and federation; and (3) the development of tutorial on risk-based cybersecurity targeted at NSF PIs and management.

The secure coding training materials have been extended to include subjects relevant to the NSF CI community: more scripting languages (expanded coverage of Perl and Python, and including Ruby), data serialization attacks, and XML attacks. This work augments related material added under other funding for C#, a major language for web and distributed systems work. The vulnerability assessment materials have been extended with several new sections, including a key "Owning the Bits" section (attacks from the point of view of the hacker), and personnel have started initial work on practical (hands on) exercises.

Building from our engagement with LIGO, CTSC developed a tutorial on identity management and federation that was initially delivered to LIGO's collaborators in India to help foster LIGO's International collaboration efforts and will be presented at the upcoming NSF Cybersecurity Summit. The tutorial does not assume any previous experience with building identity management infrastructure for scientific organizations and introduces vocabulary necessary to interact with the identity federation communities. It also discusses "lessons learned" by LIGO as it went through the process of building an identity and access management infrastructure to support a large virtual organization.

With respect to the Risk-based Cybersecurity tutorial, CTSC documented the process that it utilized for LNO, CyberGIS and IceCube, and turned that into a 4 hour long training session that educates NSF PI's 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 will debut at the NSF Cybersecurity Summit.

## 3.2 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: (1) 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 (2) 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).

During our first year, we have focused on an education module covering characteristics and security needs of scientific CI, and the key concepts relevant to the security of scientific CI such as federated identities, delegation, and single sign-on. This module is targeted at audience group 1. An initial version of this module, in particular with a focus on delegation and single sign on, is on track to be debuted in a senior level security course (CS 461/ECE 422 Computer Security I) at the University of Illinois this Fall. We will disseminate these modules freely via the CTSC website and are actively seeking additional adopters to provide feedback and improve the modules.

A module that targets audience group 2, and focuses on basic security concepts and motivate the need for security in scientific CI has also been worked on and is expected to be available in Spring 2014.

## 3.3 Summer of Networking

CTSC supports the development of skilled cybersecurity professionals and researchers by directly engaging students in stimulating cybersecurity activities. CTSC collaborated with Indiana University's successful Summer of Networking program[18] to provide cybersecurity-focused an 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 continue to work with CTSC into the Fall of 2013 as hourly research assistants.

## 3.4 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's final online outreach component is the recently established Trusted CI Forum (trustedci.groupsite.com) to support ongoing community to be established at the NSF Cybersecurity Summit.

Presentations made by CTSC were:

- Von Welch. Trustworthy Scientific Cyberinfrastructure. Presentation at NSF, July 2013. http://www.vonwelch.com/pubs/CTSC-NSF-NSF2013
- Von Welch. NSF Cybersecurity Summit. Presentation at NSF Large Facilities Security Committee, July 2013

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

- Von Welch. Trustworthy Scientific Cyberinfrastructure: Challenges and Opportunities. Presentation at USC/ISI, March 2013. http://www.vonwelch.com/pubs/CTSC-ISI-MAR2013
- Von Welch. Managing a software project - the dos and don'ts. Presentation at NSF SI2 PI Meeting, January 2013. http://www.vonwelch.com/pubs/SI2-JAN2013
- Von Welch. CACR Cyberinfrastructure Projects. Supercomputing 2012 IU Booth Presentation, November 2012. http://www.vonwelch.com/pubs/CACR-SC12

Additionally, a one-page handout on CTSC[19] was distributed at Supercomputing 2012 and the 2013 Bro Exchange.

# 4 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 leverages a broad understanding of the NSF CI community to actively seek opportunities to align cybersecurity solutions for interoperability to better support collaboration.

## 4.1 NSF Cybersecurity Summit for Cyberinfrastructure and Large Facilities

Spanning six years from 2004-2009, the NSF-funded annual Cybersecurity Summits served as a valuable part of the process of securing the NSF-funded cyberinfrastructure (CI) and MREFC projects by providing the community with the opportunity to share best practices, educate themselves from experts both from within and from outside of the community, and collaborate on solving common challenges.

Under a supplemental award, CTSC is re-launching the NSF Cybersecurity Summit for Cyberinfrastructure and Large Facilities ("the NSF Cybersecurity Summit"). The 2013 Summit is scheduled September 30 through October 2, 2013 at the Hilton Arlington near NSF headquarters. The 2013 Summit will provide training opportunities from both CTSC (Secure Coding Practices, Risk-based Cybersecurity Programs for PIs and Managers, and Streamlining Collaboration with InCommon and Identity Federations) and from the Bro Team (Network Security and Monitoring).

The plenary session will focus on refining the requirements for an NSF CI cybersecurity program and how to best foster collaboration and the sharing of best practices and lessons learned between NSF CI projects to build a coherent NSF CI cybersecurity ecosystem. The final day will

[19] http://trustedci.org/flyer

have the participants in different working groups to work on challenges identified during the plenary.

CTSC envisions the Summit as an ongoing annual event. Towards that end, CTSC has instantiated the Trusted CI Forum (https://trustedci.groupsite.com) to provide the community with a place to interact during the year between summits, and plans to re-propose a Summit to NSF next year.

## 4.2 A Risk-Based Cybersecurity Program Design Process for CI

CTSC has subscribed to a risk-based approach to the development of cybersecurity programs. What this translates into is identifying and evaluating the cybersecurity risks associated with a project and then using that work to design a cybersecurity program that fits the needs of that particular project. CTSC's approach is based off of the standard NIST 800-30[20] approach and is informed by earlier risk assessments performed by NCSA and PSC for other NSF projects including Blue Waters, XSEDE, and GENI.

CTSC has been tailoring this approach to address the challenges particular to the NSF CI community. A primary challenge is that every NSF CI project we have worked with is embedded in and leverages varying degrees of the commodity IT infrastructure, cybersecurity infrastructure and cybersecurity policies of the university or organization that hosts them. Trying to assess this entire infrastructure would be impossible with any reasonable amount of effort, and even if possible, would bear little benefit since CTSC's ability to influence this infrastructure and policies to any meaningful degree is extremely limited. Instead, CTSC is working on abstractions and best practices that cover these topics to allow CTSC (and other NSF CI projects) to reasonably include them in an assessment and cybersecurity plan without undue effort.

Additional challenges include:

- These prior assessments were significant undertakings and represented more resource hours to complete than CTSC felt we could expect 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 (universities or research laboratories) and benefit from, and are restricted by, their cybersecurity programs and commodity IT infrastructure.

[20] http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

CTSC has been honing the previously mentioned risk assessment approaches to be more streamlined, with a set of common threats and types of assets for CI projects, and methods for abstracting the complicated relationships with their underlying organizations. We expect to keep improving this approach throughout the life of CTSC, but we will be sharing our current practices and processes this Fall as a training session at the NSF Cybersecurity Summit.

## 4.3 CTSC Cybersecurity Program

CTSC itself is an NSF CI project and hence followed its own guidance and developed it's own cybersecurity program. CTSC has made its program publicly available[21], 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.

## 4.4 CTSC Whitepapers and Technical Reports

CTSC's leadership efforts include the publication of papers providing both guidance to the community and stating opinions of direction to unify community approach:

- Jim Basney and Von Welch. Science Gateway Security Recommendations. Science Gateway Institute Workshop (at IEEE Cluster 2013), September 2013. http://www.vonwelch.com/pubs/GWSecurity13
- Randy Heiland, Betsy Thomas, Von Welch and Craig Jackson. Toward a Research Software Security Maturity Model. Workshop on Sustainable Software for Science: Practice and Experiences (submitted), November 2013. http://www.vonwelch.com/pubs/WSSPE13
- Jim Basney and Von Welch. Enabling Cross-Campus Research Collaborations: The IdM Provisioning and Deployment Challenge. Identity Management Collaboration Meeting, Chicago. IL. August 2013. http://www.vonwelch.com/pubs/KeyIdM13

## 4.5 Interagency, Higher Ed 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, CTSC is maintaining strong ties with DHS activities through Welch and Basney's role as co-PIs in the DHS Software Assurance Marketplace (SWAMP), and is also in process of initiating collaborations with the UK Engineering and Physical Sciences Research Council's newly forming cybersecurity working group. We maintain good ties with the Internet2 and Higher Ed community through Basney and Koranda's participation on the

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

InCommon Technical Advisory and Assurance Advisory Committees respectively. Additionally our advisory committee, discussed in the next section, provides us with additional ties to the DOE, Internet2, higher education, and International communities.

# 5 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 established an advisory committee to help inform and steer its efforts. The committee was formed at the start of the project and met once in the first year, with a second in-person meeting scheduled in November 2013 at Supercomputing 13 in Denver.

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/.

# 6 Year 1 Lessons Learned and Challenges

CTSC has identified a number of lessons learned and ongoing challenges in its first year (in no particular order):

- Practice makes perfect: While CTSC consists of cybersecurity professionals who have undertaken many risk assessments and developed numerous cybersecurity plans over their careers, CTSC provides an opportunity to perform those tasks with a frequency and level of collaboration that would not otherwise exist. This provides the opportunity to

experiment with different techniques and determine what approaches best serve the NSF CI community.

- Tension of sharing: 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 hope the Trusted CI Forum will provide projects with sufficient privacy to make them comfortable with sharing these products.
- Importance of engagement planning: Before undertaking the technical work involved in a collaboration, CTSC develops an engagement plan in consultation with the engaged project. This document has proven invaluable in ensuring the scope, timeline, committed resources and outcomes are well understood by both parties.
- Challenge of community IT and underlying organizations: As we described previously, every NSF CI project we have worked with is embedded in and leverages varying degrees of the commodity IT infrastructure, cybersecurity infrastructure and cybersecurity policies of the university or organization that hosts them. CTSC is working on abstractions and best practices that cover these topics to allow CTSC (and other NSF CI projects) to reasonably include them in an assessment and cybersecurity plan without undue effort.
- Engagement Impact Metrics: We continue to wrestle with appropriate impact metrics for the engagements. Our collection of statements from the projects for this report was an initial attempt, but we suspect it was premature to gauge impact from the engagements as insufficient time had passed to make impact clear.

# 7 Year 2 Plans

In this section we describe CTSC's plans for project year 2 (Oct 1, 2013 - Sep 30, 2014).

## 7.1 Engagements

CTSC will continue to spend the majority of its effort on engagements with NSF CI projects to address their cybersecurity challenges. At the upcoming NSF Cybersecurity Summit, CTSC will announce an open call for projects to request an engagement with CTSC. In our proposal and subsequent revised statement of work, we indicated we would undertake four engagements in year two, a number we plan to easily surpass given our completion of three and our substantial progress on four more engagements in year one.

In addition to these larger engagements, CTSC recognizes a need for shorter, informal interactions with projects that may turn into a longer engagement or may satisfy a project's need in itself. We will experiment with offering these lighter-weight engagements by allowing projects to ask questions or undertake "expert access" phone calls or meetings with projects.

## 7.2 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 within year one to solicit feedback on how our engagement impacted the project once some time has passed.

## 7.3 Education, Outreach and Training

In year two the training program will focus its efforts on refining our newly created identity management and cybersecurity program tutorials and finding more venues to deliver them (we plan on revisiting XSEDE and Supercomputing, as well as exploring options such as the NSF Large Facilities workshop[22] and the SI2 PI meeting). The University of Wisconsin team will concentrate in the coming year on 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.

We will also investigate the electronic delivery of this material with the goal of making at least one of these tutorials available for on-demand access by the community, as well as augmenting it with a list of other training resources from the broader community of use to the CI community and made it available on the CTSC website.

NSF recently funded a major new security initiative focused on network security and monitoring (PIs: Sommer and Slagell). This area of training will be a major focus for collaboration between these two groups, both in terms of sharing material and coordinating venues. We note that the two teams are already collaborating on training at the upcoming 2013 NSF Cybersecurity Summit.

Education activities in year 2 will see the continued development of education modules targeting audience group 1 with emphasis placed on the security technologies currently in use and under development for scientific CI. Lessons learned and feedback obtained from the use of modules in the senior level computer security course at the University of Illinois will inform the development of these education modules in year 2. We also plan to complete the development of education modules targeted at audience group 2 (students who are end users of CI, but who may not necessarily have a background in security) and debut them in a course. We are currently working to identify such a course both at and outside CTSC partner institutions.

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.

[22] https://science.nrao.edu/science/meetings/2013-nsf-large-facility-operations-workshop

## 7.4 NSF Cybersecurity Summit and Trusted CI Forum

Our vision is for the NSF Cybersecurity Summit and the Trusted CI Forum to serve as an ongoing platform for the NSF CI Community to collaborate on cybersecurity. CTSC will continue to operate and manage the Forum and we plan on making a proposal to NSF for further supplemental funds to host another Forum in 2014.

## 7.5 State of NSF Cybersecurity Report

CTSC's plan to create an annual report on the state of practice of cybersecurity in the NSF scientific CI community in year one was delayed to take advantage of the results we expect to emerge from the NSF Cybersecurity Summit. We plan to either integrate this report with the Cybersecurity Summit report (if that integration works) or publish it separately by the end of 2013. This report will contains a gap analysis that documents key challenges and missing functionality, as well as major changes to the cybersecurity ecosystem over the past year. The report will be disseminated on the CTSC website.

# 8 Conclusion

CTSC has had a very successful year one with three engagements completed, three nearly completed and a seventh already initiated. We are developing a risk assessment and cybersecurity planning process for NSF CI Cybersecurity programs that incorporates well-known best practices as well as tackles NSF CI challenges of being embedded in other organizations, and handling their unique instruments and data assets. We have successfully relaunched and organized the NSF Cybersecurity Summit along with a Trusted CI Forum to foster an ongoing NSF community focused on NSF CI cybersecurity. Leveraging prior training materials from the University of Wisconsin team and creating two new tutorials, we delivered seven training sessions. Educational activities included creating a new education module on cybersecurity for CI that is being utilized in a class at the University of Illinois this Fall, mentoring of a student in Indiana University's Summer of Networking program and the ongoing membership of two students in the CTSC team as research assistants. Our broader impacts include the publication of engagement products and three other papers to define community best practices.

# References

[1] 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: http://hdl.handle.net/2022/14174 [cited 12 Feb 2012]

[2] 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, pp. 219-237.

[3] 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

[4] Basney, J., Koranda, S., "Center for Trustworthy Scientific Cyberinfrastructure Engagement Plan: Final Report for LIGO Engagement," July, 2013. Available: http://hdl.handle.net/2022/16689

[5] Basney, J., Koranda, S., "A Study of Three Approaches to International Identity Federation for the LIGO Project," July, 2013. Available: http://hdl.handle.net/2022/16760

[6] Basney, Jim; Koranda, Scott. "InCommon Membership in eduGAIN: the LIGO Perspective," May, 2013. Available: http://hdl.handle.net/2022/16690