CTSC

CENTER FOR TRUSTWORTHY
SCIENTIFIC CYBERINFRASTRUCTURE

The NSF Cybersecurity Center of Excellence

The NSF Cybersecurity Center of Excellence: Current and Future Large Facilities Impacts

James A. Marsteller

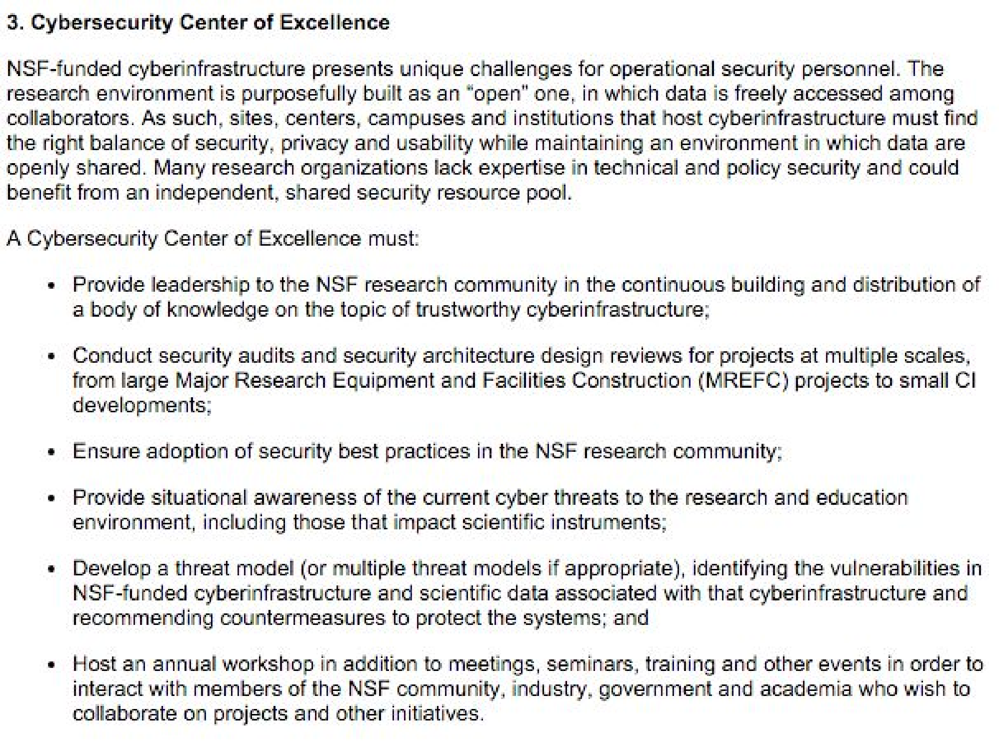
NSF Large Facilities Workshop
May 3rd 2017

trustedci.org

NSF Cybersecurity Center of Excellence (CCoE)

CTSC began with a 3-year NSF grant in 2012.

Re-funded in 2015 for 3 years by ACI/OAC Cybersecurity Innovation for Cyberinfrastructure (CICI) solicitation.



3. Cybersecurity Center of Excellence

NSF-funded cyberinfrastructure presents unique challenges for operational security personnel. The research environment is purposefully built as an "open" one, in which data is freely accessed among collaborators. As such, sites, centers, campuses and institutions that host cyberinfrastructure must find the right balance of security, privacy and usability while maintaining an environment in which data are openly shared. Many research organizations lack expertise in technical and policy security and could benefit from an independent, shared security resource pool.

A Cybersecurity Center of Excellence must:

- Provide leadership to the NSF research community in the continuous building and distribution of a body of knowledge on the topic of trustworthy cyberinfrastructure;
- Conduct security audits and security architecture design reviews for projects at multiple scales, from large Major Research Equipment and Facilities Construction (MREFC) projects to small CI developments;
- Ensure adoption of security best practices in the NSF research community;
- Provide situational awareness of the current cyber threats to the research and education environment, including those that impact scientific instruments;
- Develop a threat model (or multiple threat models if appropriate), identifying the vulnerabilities in NSF-funded cyberinfrastructure and scientific data associated with that cyberinfrastructure and recommending countermeasures to protect the systems; and
- Host an annual workshop in addition to meetings, seminars, training and other events in order to interact with members of the NSF community, industry, government and academia who wish to collaborate on projects and other initiatives.

http://www.nsf.gov/pubs/2015/nsf15549/nsf15549.htm http://trustedci.org/who-we-are/

CTSC
CENTER FOR TRUSTWORTHY SCIENTIFIC CYBERINFRASTRUCTURE
The NSF Cybersecurity Center of Excellence

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

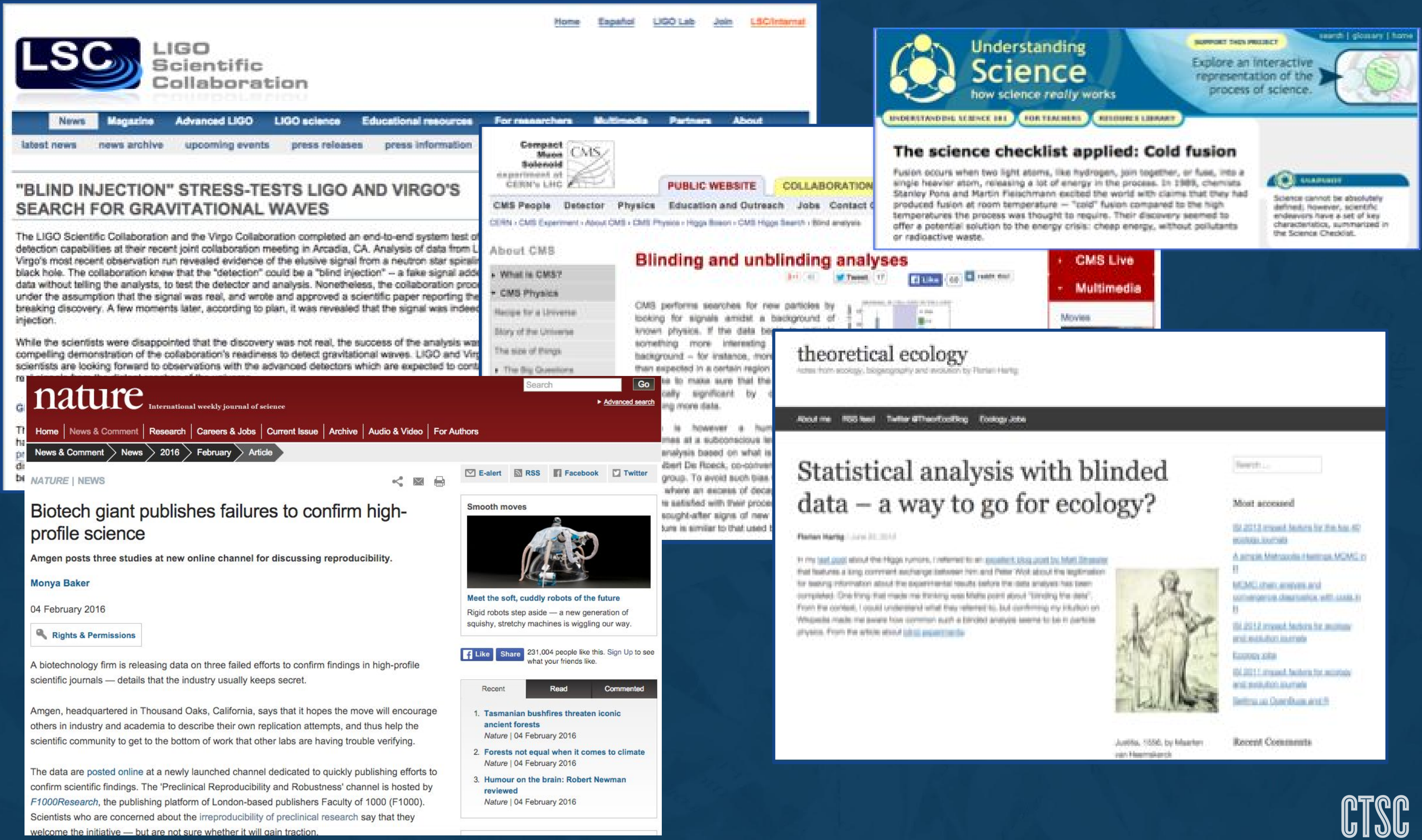
NCSA

PITTSBURGH SUPERCOMPUTING CENTER

THE UNIVERSITY of WISCONSIN
MADISON

NSF

Why Cybersecurity Matters?
Trusted and Reproducible Science



"BLIND INJECTION" STRESS-TESTS LIGO AND VIRGO'S SEARCH FOR GRAVITATIONAL WAVES

The LIGO Scientific Collaboration and the Virgo Collaboration completed an end-to-end system test of detection capabilities at their recent joint collaboration meeting in Arcadia, CA. Analysis of data from L Virgo's most recent observation run revealed evidence of the elusive signal from a neutron star spirali black hole. The collaboration knew that the "detection" could be a "blind injection" – a fake signal adde data without telling the analysts, to test the detector and analysis. Nonetheless, the collaboration proc under the assumption that the signal was real, and wrote and approved a scientific paper reporting the breaking discovery. A few moments later, according to plan, it was revealed that the signal was indeed injection.

While the scientists were disappointed that the discovery was not real, the success of the analysis wa compelling demonstration of the collaboration's readiness to detect gravitational waves. LIGO and Vir scientists are looking forward to observations with the advanced detectors which are expected to con

Blinding and unblinding analyses

CMS performs searches for new particles by looking for signals amidst a background of known physics. If the data be something more interesting background – for instance, more than expected in a certain region

is however a hum at a subconscious le analysis based on what is lbert De Roeck, co-conve group. To avoid such bias where an excess of deca is satisfied with their proce sought-after signs of new ture is similar to that used

The science checklist applied: Cold fusion

Fusion occurs when two light atoms, like hydrogen, join together, or fuse, into a single heavier atom, releasing a lot of energy in the process. In 1989, chemists Stanley Pons and Martin Fleischmann excited the world with claims that they had produced fusion at room temperature — "cold" fusion compared to the high temperatures the process was thought to require. Their discovery seemed to offer a potential solution to the energy crisis: cheap energy, without pollutants or radioactive waste.

Science cannot be absolutely defined; however, scientific endeavors have a set of key characteristics, summarized in the Science Checklist.

NATURE | NEWS

Biotech giant publishes failures to confirm high-profile science

Amgen posts three studies at new online channel for discussing reproducibility.

Monya Baker

04 February 2016

Rights & Permissions

A biotechnology firm is releasing data on three failed efforts to confirm findings in high-profile scientific journals — details that the industry usually keeps secret.

Amgen, headquartered in Thousand Oaks, California, says that it hopes the move will encourage others in industry and academia to describe their own replication attempts, and thus help the scientific community to get to the bottom of work that other labs are having trouble verifying.

The data are posted online at a newly launched channel dedicated to quickly publishing efforts to confirm scientific findings. The 'Preclinical Reproducibility and Robustness' channel is hosted by *F1000Research*, the publishing platform of London-based publishers Faculty of 1000 (F1000). Scientists who are concerned about the irreproducibility of preclinical research say that they welcome the initiative — but are not sure whether it will gain traction.

Smooth moves

Meet the soft, cuddly robots of the future

Rigid robots step aside — a new generation of squishy, stretchy machines is wiggling our way.

231,004 people like this. Sign Up to see what your friends like.

1. Tasmanian bushfires threaten iconic ancient forests
   Nature | 04 February 2016
2. Forests not equal when it comes to climate
   Nature | 04 February 2016
3. Humour on the brain: Robert Newman reviewed
   Nature | 04 February 2016

Statistical analysis with blinded data – a way to go for ecology?

Florian Hartig | June 22, 2012

In my last post about the Higgs rumors, I referred to an excellent blog post by Matt Strassler that features a long comment exchange between him and Peter Woit about the legitimation for leaking information about the experimental results before the data analyses has been completed. One thing that made me thinking was Matts point about "blinding the data". From the context, I could understand what they referred to, but confirming my intuition on Wikipedia made me aware how common such a blinded analysis seems to be in particle physics. From the article about blind experiments:

Justitia, 1556, by Maarten van Heemskerck

Most accessed

- ISI 2013 impact factors for the top 40 ecology journals
- A simple Metropolis-Hastings MCMC in R
- MCMC chain analysis and convergence diagnostics with coda in R
- ISI 2012 impact factors for ecology and evolution journals
- Ecology jobs
- ISI 2011 impact factors for ecology and evolution journals
- Setting up OpenBugs and R

Recent Comments

Caution:
“Our data is public” doesn’t save the day

Reputation, trust, and other “intangibles” matter.

Integrity and availability of data

Illicit use of systems

Availability of instruments

Hacktivism

Etc.

Center for Trustworthy Cyberinfrastructure
The NSF Cybersecurity Center of Excellence

Mission

Provide the NSF community a coherent understanding of cybersecurity’s role in producing trustworthy science and the information and know-how required to achieve and maintain effective cybersecurity programs.

Vision for the NSF Science Community

1. For the NSF science community to understand fully the role of cybersecurity in producing trustworthy science.

2. For all NSF projects and facilities to have the information and resources they need to build and maintain effective cybersecurity programs appropriate for their science missions, and responsive to evolving risks and requirements.

3. For all NSF Large Facilities to have highly effective cybersecurity programs.

CCoE Thrusts

Building Community

NSF Cybersecurity Summit, Monthly Webinars, Blog, Email Lists, Partnerships, Benchmarking Survey, LFs Security WG

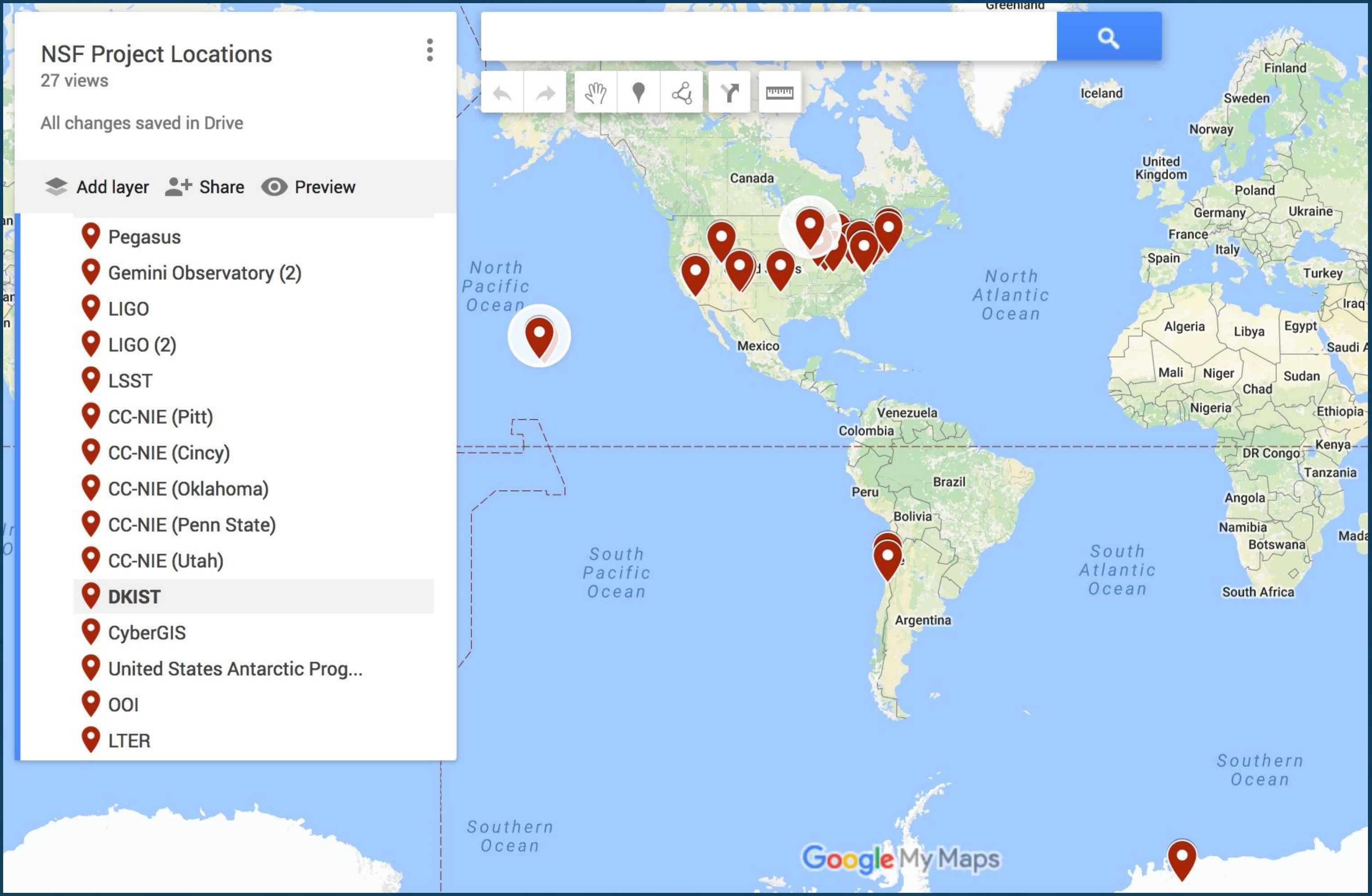
Sharing Knowledge

Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects, Identity Management Best Practices, Situational Awareness, Training, OSCRP

Collaboration to Tackle Challenges: Engagements (LFs)

LIGO, SciGaP, IceCube, Pegasus, CC-NIE peer review, DKIST, LTERNO, DataONE, SEAD, CyberGIS, HUBzero, Globus, LSST, NEON, U. Utah, PSU, OOI, Gemini, Array of Things, IBEIS, SciGaP, US Antarctic Program...

CCoE Engagement Map



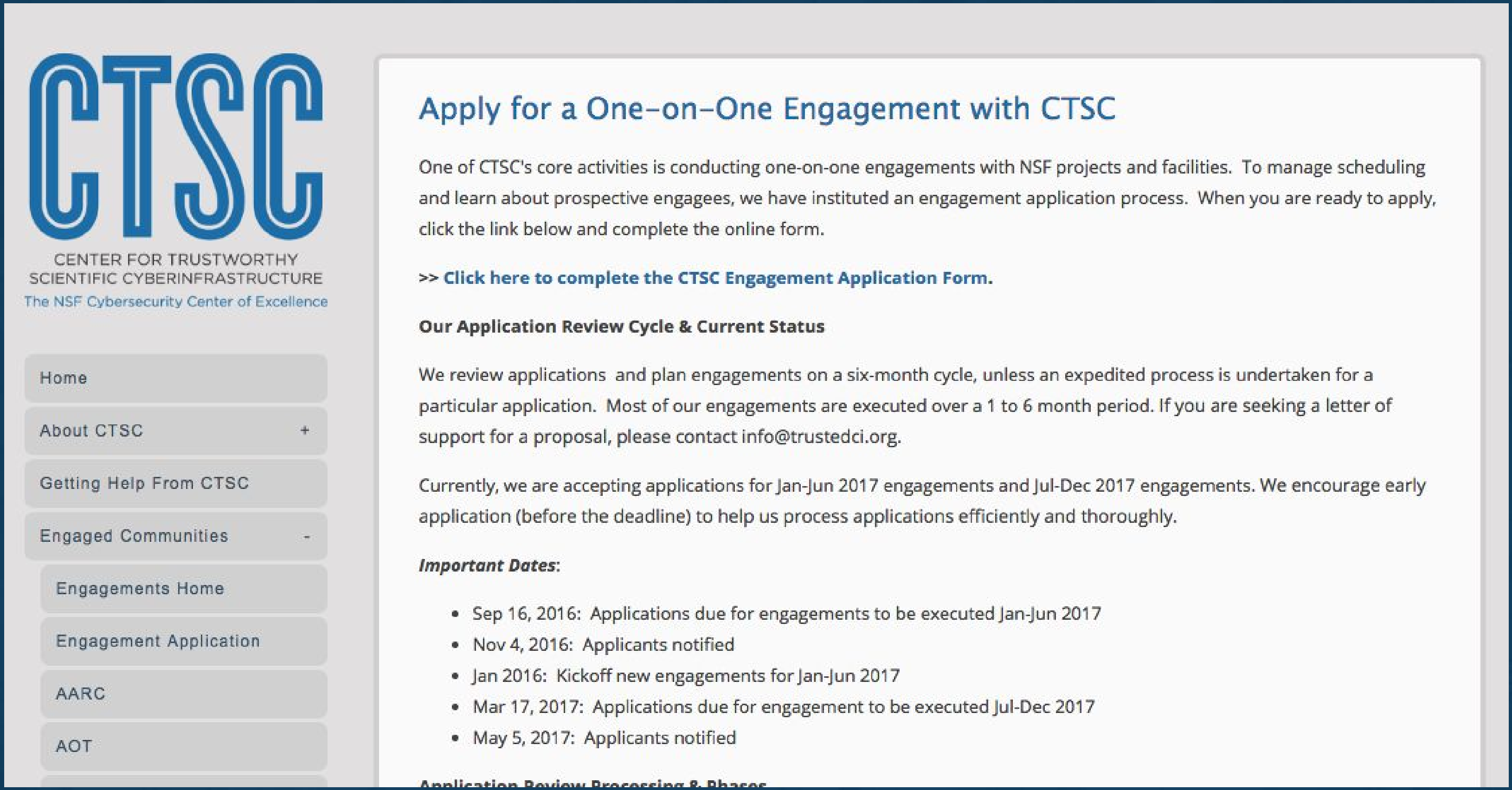
NSF Project Locations

27 views

All changes saved in Drive

Add layer Share Preview

- Pegasus
- Gemini Observatory (2)
- LIGO
- LIGO (2)
- LSST
- CC-NIE (Pitt)
- CC-NIE (Cincy)
- CC-NIE (Oklahoma)
- CC-NIE (Penn State)
- CC-NIE (Utah)
- **DKIST**
- CyberGIS
- United States Antarctic Prog...
- OOI
- LTER



Apply for a One-on-One Engagement with CTSC

One of CTSC's core activities is conducting one-on-one engagements with NSF projects and facilities. To manage scheduling and learn about prospective engagees, we have instituted an engagement application process. When you are ready to apply, click the link below and complete the online form.

>> **Click here to complete the CTSC Engagement Application Form.**

Our Application Review Cycle & Current Status

We review applications and plan engagements on a six-month cycle, unless an expedited process is undertaken for a particular application. Most of our engagements are executed over a 1 to 6 month period. If you are seeking a letter of support for a proposal, please contact info@trustedci.org.

Currently, we are accepting applications for Jan-Jun 2017 engagements and Jul-Dec 2017 engagements. We encourage early application (before the deadline) to help us process applications efficiently and thoroughly.

Important Dates:

- Sep 16, 2016: Applications due for engagements to be executed Jan-Jun 2017
- Nov 4, 2016: Applicants notified
- Jan 2016: Kickoff new engagements for Jan-Jun 2017
- Mar 17, 2017: Applications due for engagement to be executed Jul-Dec 2017
- May 5, 2017: Applicants notified

Application Review Processing & Phases

http://trustedci.org/application

Demand outpaces Supply: March 17th Deadline for 2017Q3-4 engagements.

Activities Impacting the NSF Large Facilities

NSF Large Facilities:

Orange: CTSC Past Engagee

Academic Research Fleet ARF
Antarctic Infrastructure Modernization for Science AIMS
Arecibo Observatory AO
Atacama Large Millimeter/submillimeter Array ALMA
Cornell Laboratory for Accelerator-based Science and Education CLASS
Daniel K. Inouye Solar Telescope DKIST
Gemini Observatory GEMINI
Geodetic Facilities for Advancement of Geoscience & EarthScope GAGE
Green Bank Observatory GBO
IceCube South Pole Neutrino Observatory IceCube
JOIDES Resolution International Ocean Discovery Program JOIDES
Large Hadron Collider LHC
Large Synoptic Survey Telescope LSST
Laser Inferometer Gravitational-Wave Observatory LIGO
Long Term Ecological Research Network LTER
National Center for Atmospheric Research NCAR

Green: Need to Connect

National Ecological Observatory Network NEON
National Geophysical Observatory for Geoscience NEGO
National High Magnetic Field Laboratory NHMFL
National Nanotechnology Coordinated Infrastructure NNCI
National Nanotechnology Infrastructure Network NNIN
National Optical Astronomy Observatory NOAO
National Radio Astronomy Observatory NRAO
National Solar Observatory NSO
National Superconducting Cyclotron Laboratory NSCL
Natural Hazards Engineering Research Infrastructure NHERI
Ocean Observatories Initiative OOI
Polar Facilities and Logistics
Seismology Facilities for Advancement of Geoscience & EarthScope SAGE

Large Facilities Security Working Group

Proposed to FacSec 9/2016 - “ To develop a relationship between those responsible for cybersecurity across the LFs and to advance the development and implementation of best practices, standards and requirements within the CI community.”

- First meeting on January 26th 2017
  - Attended: Ice Cube, CMS, LIGO, LSST, NHMFL NOAO
  - Established LF Security mailing list
- Monthly calls
- Develop lines of Communication / Build Community

Large Facilities Security Working Group

Current Goals:

- Provide critical input on LF software requirements for software producers.
- LF participation in CCoE Situational Awareness initiative (90% by LFs by 2019).
- Increase CTSC's awareness of current issues, challenges, and successes at the LFs.

Large Facilities Security Working Group

Current Goals:

- Build consensus so we can, where feasible, communicate with a unified voice.
- Engage LF Security working group for input on the Guide, Community Survey, Training needs and other topics as needed.
- Provide feedback and input on the Cybersecurity subsection of the large facilities manual.

Large Facilities Security Working Group

USAP		**NCAR**	Jose Castilleja
Arecibo		**NHERI**	Nathaniel Mendoza
Academic Fleet		**NEON**	Tom Gulbransen, Rick Fransworth
CHESS		**SAGE**	
Green Bank		**GAGE**	
Gemini	Chris Morrison	**NHMFL**	Peter Jensen
Ice Cube	Steve Barnet	**NNCI**	
IODP (Joides Resolution)		**NOAO**	Steve Grandi
LBO		**NRAO**	Patrick Murphy
LHC/ATLAS		**NSCL**	
LHC/CMS	Mine Altunay	**NSO**	Eric Cross, Shawn Granen
LIGO	Randy Trudeau	**OOI**	Juan jose Villalobos, Ivan Rodero
LSST	Alex Withers		

NSF Cybersecurity Summit

- Inaugural summit in 2004 in response to cyber attack affecting many NSF funded projects
- CTSC Relaunched Summit in 2013 after 4 year hiatus
- Opportunity for CI, MREFCs to collaborate: solve common challenges, develop best practices, share experiences/knowledge, training sessions
- Who: NSF POs, LF leadership, Researchers, IT staff
- Help to address the changing threat landscape for NSF CI

NSF Cybersecurity Summits

- 2016 Summit
  - 98% of respondents selected “Good” or “Excellent.”
  - Best CFP response to date (19 proposals)
  - Summit Report published to community on http://trustedci.org/2016summit

- 2017 Summit
  - Dates selected: August 15-17
  - CFP and Student Program Announced
  - 2018 Summit in Alexandria

2017 Summit Call For Participation (CFP)

Now accepting community proposals:

- Plenary Presentations
- Training Sessions
- Table Talk Sessions
- Student Program
- CFP Deadline June 5th

Seeking CFPs addressing:

- Lessons Learned
- Budgeting for Cybersecurity
- Cybersecurity Metrics
- Risk Acceptance Practices
- Software Assurance

Email CFPs (1-5 pages) to CFP@trustedci.org

More information: http:/trustedci.org/2017-nsf-cfp/

2017 NSF Cybersecurity Summit:

August 15-17, 2016 - Arlington, Virginia

http://trustedci.org/summit

Software Security

- Generally: Feedback from Large Facilities to CI development community would be useful.
  - What services would be useful?
  - How can they be developed to be most useful?

- Community standards for production software development are lacking, particularly for security.
  - E.g. assurance, patching, testing

- CTSC will convene Large Facilities and software developers (e.g. SI2) to determine reasonable expectations for production software security.

Situational Awareness

Advise NSF CI community about relevant software vulnerabilities and provide guidance on mitigation.

Leverage NIST, US-CERT, XSEDE, REN-ISAC, and other sources of vulnerability information.

Currently eight identified Large Facilities subscribed.

http://trustedci.org/situational-awareness/

Cybersecurity Guidance for Large Facilities

- NSF Large Facilities Manual currently has minimal guidance on cybersecurity (Section 5.3)
    - https://www.nsf.gov/bfa/lfo/lfo_documents.jsp
- CTSC drafted guidance based on our engagements with Large Facilities
- Have shared with NSF Large Facilities Office. Will share with Large Facilities Security WG and broader community.
- Guidance is freely available for use by Large Facilities and NSF LFO.

NSF Community Cybersecurity Benchmarking Survey

trustedci.org/survey

Goal: To produce a report on the aggregated state of cybersecurity across the community and track the improvement of that state over time.

Plan to repeat annually with community support.

Nine large facilities responded in 2016.

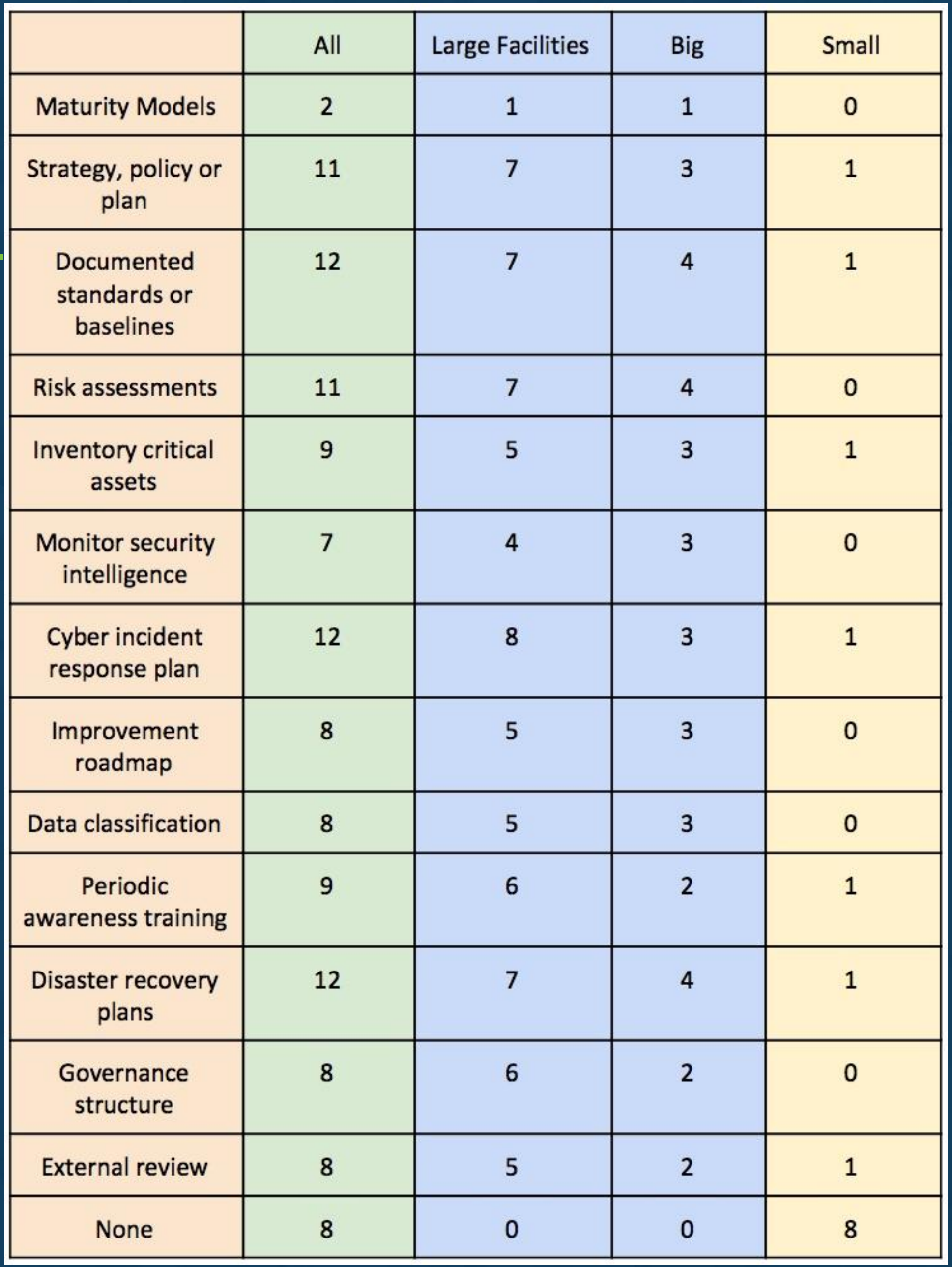
NSF Community Cybersecurity Benchmarking Survey Findings:

- Security budgets: Large Facilities range from 0.02% - 1.5% of annual budget.
- Big projects range from 0.25% - 4.58% of annual budget
  - Average cybersecurity budget as a percentage of IT budget sits at the low end of the average values found in industry.
- Few respondents produce inventories of critical systems or use data classification scheme.
- Most respondents with annual budgets above $1M detected cybersecurity incidents in past year (Large Facilities - 7 of 9)

NSF Community Cybersecurity Benchmarking Survey Findings:

- Large Facility respondents indicate a greater concern than respondents in the other categories for threats of sabotage or other events affecting availability of critical systems.
- All respondents reported that they develop software in house.
- Nearly all respondents undertake some cybersecurity policy development. However, several respondents, including 3 of 16 with >$1m dollar budgets, do not employ a framework or identified guidance resource to help shape the cybersecurity program.
- Many projects do not have process for accepting residual information security risk.

What programmatic cybersecurity safeguards has your project or facility implemented?



	All	Large Facilities	Big	Small
Maturity Models	2	1	1	0
Strategy, policy or plan	11	7	3	1
Documented standards or baselines	12	7	4	1
Risk assessments	11	7	4	0
Inventory critical assets	9	5	3	1
Monitor security intelligence	7	4	3	0
Cyber incident response plan	12	8	3	1
Improvement roadmap	8	5	3	0
Data classification	8	5	3	0
Periodic awareness training	9	6	2	1
Disaster recovery plans	12	7	4	1
Governance structure	8	6	2	0
External review	8	5	2	1
None	8	0	0	8

NSF Community Cybersecurity Benchmarking Survey

Looking ahead, CTSC will use this report to fuel discussions and inform its services. Moreover, we will look for community feedback on whether to conduct a survey in 2017 and, if so, how to improve it.

View the complete community cybersecurity survey report: http://hdl.handle.net/2022/21355

Staying in contact with the CCoE

Join our email lists for discussions and updates:

http://trustedci.org/ctsc-email-lists/

Blog: http://blog.trustedci.org/

Twitter: @TrustedCI

CTSC

CENTER FOR TRUSTWORTHY
SCIENTIFIC CYBERINFRASTRUCTURE

The NSF Cybersecurity Center of Excellence

Thank You

trustedci.org

We thank the National Science Foundation (grant 1547272) for supporting our work.

The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.