



CENTER FOR TRUSTWORTHY
SCIENTIFIC CYBERINFRASTRUCTURE
The NSF Cybersecurity Center of Excellence

The NSF Cybersecurity Center of Excellence and Large Facility Cybersecurity

James A. Marsteller
NSF Large Facilities Workshop
25 May 2016

trustedci.org

Center for Trustworthy Cyberinfrastructure

The NSF Cybersecurity Center of Excellence

The mission of CTSC is to provide the NSF community with a coherent understanding of cybersecurity, its importance to computational science, and what is needed to achieve and maintain an appropriate cybersecurity program.



**CENTER FOR APPLIED
CYBERSECURITY RESEARCH**

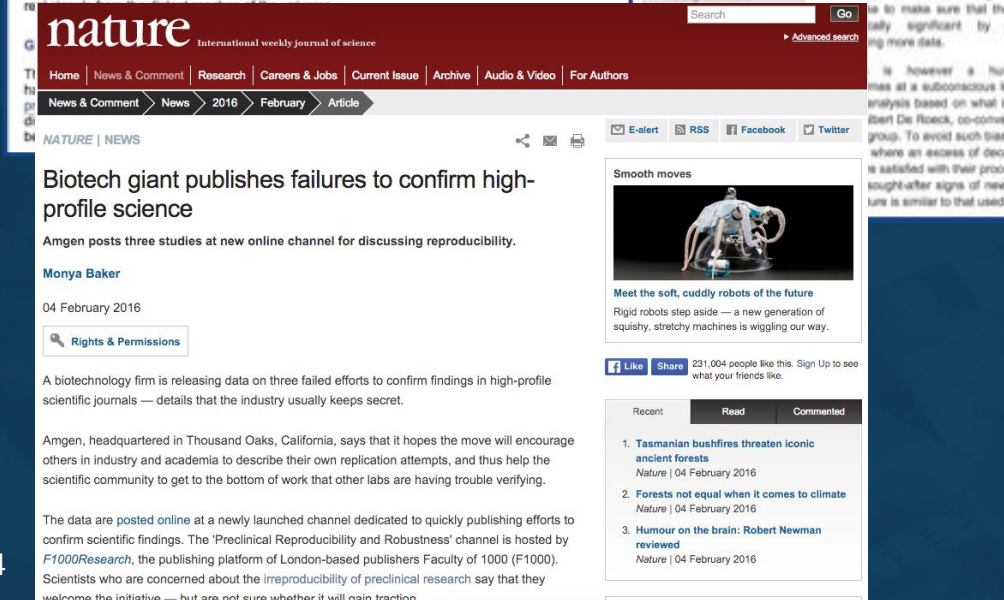
INDIANA UNIVERSITY
Pervasive Technology Institute



The Cybersecurity Challenge to NSF Science



Science Must be Trusted and Reproducible



Our IT World is Stormy

Anthem

Home FAQ A Letter from our CEO En Español

How to Access & Sign Up For Identity Theft Repair & Credit Monitoring Services

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Hackers Remotely Kill a Jeep on the Highway—With Me in It

CNBC

HOME U.S. NEWS MARKETS INVESTING TECH SMALL B

HACKING AMERICA

FBI: Computer expert briefly made plane fly sideways

Nasa hack: AnonSec attempts to crash \$222m drone, releases secret flight videos and employee data

By Mary-Ann Russon

February 1, 2016 13:05 GMT

2,127



engadget

Thirty Meter Telescope's website was hacked to protest its construction

by Mariella Moon | @mariella_moon | April 28th 2015 At 4



The Washington Post

PM databases used 22.1 million people, authorities say

Digital subscriptions SUBSCRIBE

Symantec Security

Symantec Official Blog

Digital Extortion Rise

By: Roger Park SYMANTEC EMPLOYE

Created 20 Apr 2015

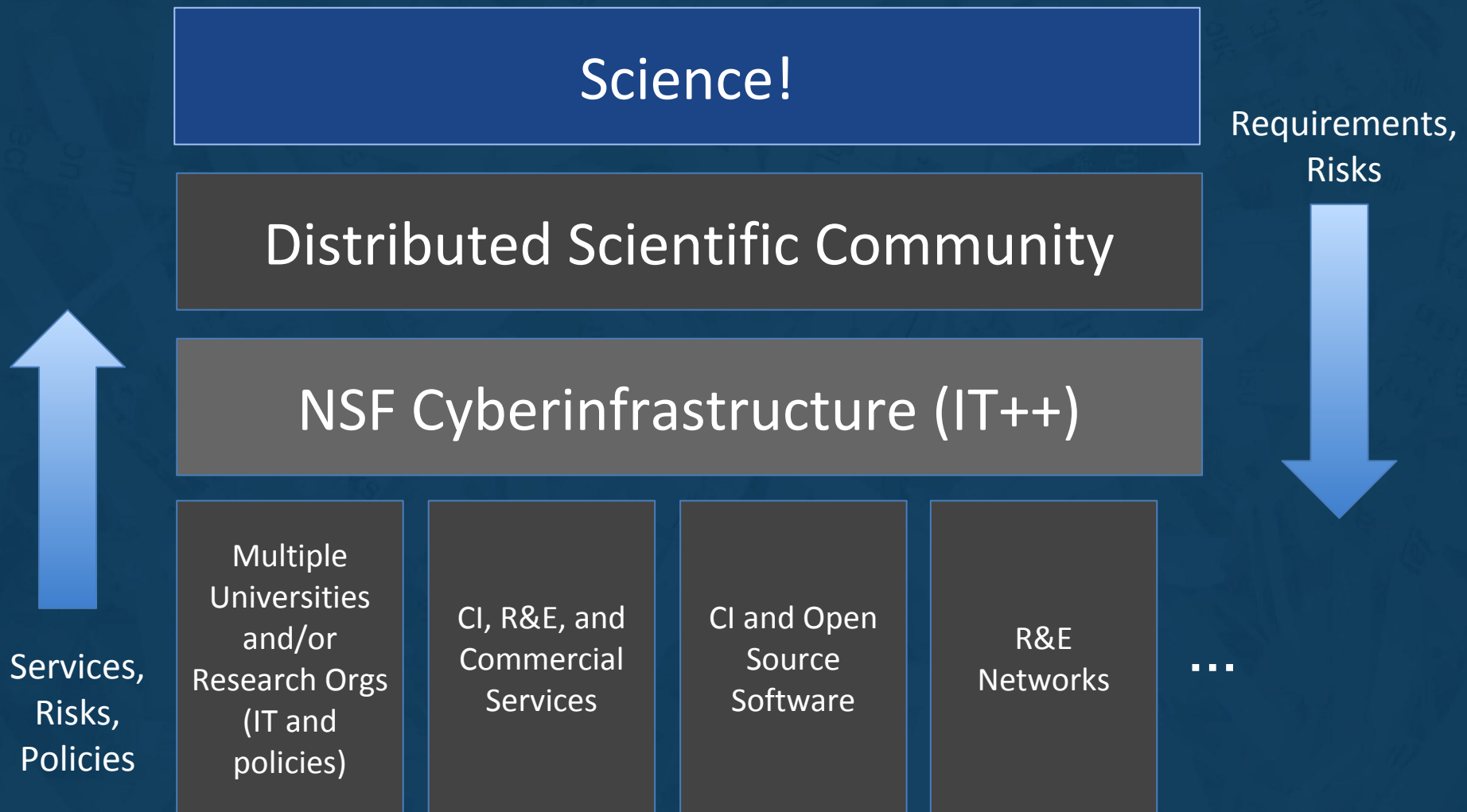
engadget

Old Intel chips are vulnerable to a fresh security exploit

by Jon Fingas | @jonfingas | August 8th 2015 At 10:11pm



Science Happens on a Complicated Ecosystem



Cybersecurity + Science Workforce?

Forbes / Tech

Top 20 Stocks for 2016

JAN 2, 2016 @ 09:06 AM 81,800 VIEWS

One Million Cybersecurity Job Openings In 2016



Steve Morgan, CONTRIBUTOR

I write about the business of cybersecurity.

[FOLLOW ON FORBES \(14\)](#)



Opinions expressed by Forbes Contributors are their own.

[FULL BIO](#) ▾



How does computational science navigate all of this?



Cybersecurity Programmatic Goal

Minimize:

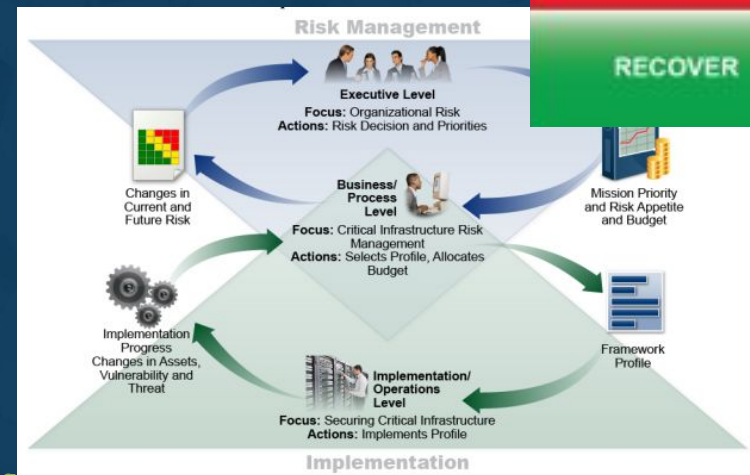
Cost of breaches/incidents

+

Cost of cybersecurity program

+

Negative impact on science productivity



Test paraphrased from: "The Defender's Dilemma. Charting a course toward Cybersecurity" http://www.rand.org/pubs/research_reports/RR1024.html

Images from NIST's "Framework for Improving Critical Infrastructure Cybersecurity"

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

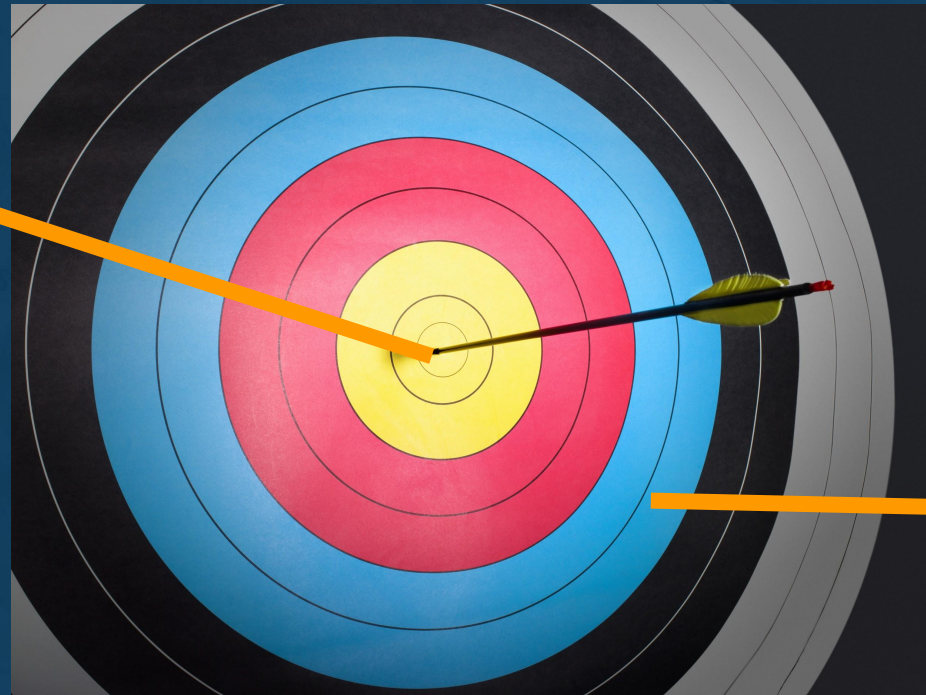
Hacktivism

Etc.

Understand where to focus

Know key liabilities and assets critical to science mission and can put focus there.

Critical assets.
Deep thinking here.



Non-critical assets.
Apply baseline controls and practices

NSF Cybersecurity Center of Excellence (CCoE)

NSF 2015
Cybersecurity
Innovation for
Cyberinfrastructure
(CICI) solicitation
created the NSF
CCoE.

CTSC submitted a
proposal and was
awarded this
honor.

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>

CTSC Activities

Engagements (LF)

LIGO, SciGAP, IceCube, Pegasus, CC-NIE peer review, DKIST, LTERNO, DataONE, SEAD, CyberGIS, HUBzero, Globus, LSST, NEON, U. Utah, PSU, OOI, U. Oklahoma, Gemini....

Education, Outreach and Training

Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects, Securing Commodity IT in Scientific CI Projects Baseline Controls and Best Practices, Training for CI professionals.

Leadership

Organized 2013, 2014 & 2015 Cybersecurity Summits for Large Facilities and CI, Incident response, Identity Management.

New CTSC Activities as CCoE

Expanded situational awareness service

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

(Large Facility participation requested - more on this later!)

Annual community benchmarking survey

Software assurance

<http://trustedci.org/software-assurance/>

Threat model for open science

<http://trustedci.github.io/OSCTP/>

Tailoring resources for smaller / newer projects

Identity and access management (IAM)

<http://trustedci.org/iam/>

CTSC Goals as a CCoE

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 Large Facilities to have highly effective cybersecurity programs.

CTSC & Large Facilities

Our Strategic 3-Year Goal for LFs

For all Large Facilities to have highly effective cybersecurity programs

Let's unpack this.

For **all** Large Facilities to have highly effective cybersecurity programs.

- As of May 2016, there are 28 LFs listed on the LFO's site. <https://nsf.gov/bfa/lfo/>
- We've had contact (engagements, summit) with 21 of the LFs.
- That leaves 7 LFs with whom we have not had an opportunity to engage or interact, or we remain unsure of how/whether to reach out....

For **all** Large Facilities to have highly effective cybersecurity programs.

We've not yet developed a relationship with:

1. Arecibo Observatory (AO)
2. Academic Research Fleet (ARF)
3. Alaska Region Research Vessel (ARRV)
4. Regional Class Research Vessel (RCRV)
5. Geodesy Advancing Geosciences and EarthScope (GAGE)
6. National Nanotechnology Coordinated Infrastructure (NNCI)
7. Seismological Facilities for the Advancement of Geosciences and EarthScope (SAGE)

For **all** Large Facilities to have highly effective cybersecurity programs.

Bottom line:

We think we can and should be interacting with all the LFs.

For all Large Facilities to have highly effective cybersecurity **programs**.

The Information Security article of the Cooperative Agreement Supplemental Financial & Administrative Terms and Conditions (CA-FATC) calls for a written summary describing a program.

In our own practice and in working with LF's, the “program” concept has been critically helpful in structuring ongoing security activities and projects.

Security for all information technology (IT) systems employed in the performance of this award, including equipment and information, is the awardee's responsibility. Within a time mutually agreed upon by the awardee and the cognizant NSF Program Officer, the awardee shall provide a **written Summary** of the policies, procedures, and practices employed by the awardee's organization as part of the organization's **IT security program, in place or planned**, to protect research and education activities in support of the award.

The Summary **shall describe the information security program appropriate for the project including, but not limited to**: roles and responsibilities, risk assessment, technical safeguards, administrative safeguards, physical safeguards, policies and procedures, awareness and training, and notification procedures in the event of a cyber-security breach. The Summary shall include the institution's evaluation criteria that will measure the successful implementation of the IT Security Program. In addition, the Summary shall address appropriate security measures required of all subawardees, subcontractors, researchers and others who will have access to the systems employed in support of this award.

The Summary will be the basis of a dialogue which NSF will have with the awardee, directly or through community meetings. Discussions will address a number of topics, such as, but not limited to, evolving security concerns and concomitant cyber-security policy and procedures within the government and at awardees' institutions, available education and training activities in cyber-security, and coordination activities among NSF awardees.

How do facilities go from having a program to have **highly effective** cybersecurity program?

For all Large Facilities to have **highly effective** cybersecurity programs.

Large Facilities Manual: NSF 15-089 (June 2015)

5.3 Guidelines for Cyber-Security of NSF's Large Facilities

“NSF has responsibility for oversight of facilities it constructs and operates, including associated IT Infrastructure. This section, **to be written**, will describe **what NSF considers to be a fundamental set of IT security requirements that facilities should consider in developing and deploying their IT plans, policies and procedures**. These **minimal requirements** and their associated evaluation criteria, as provided by the facility and agreed to by NSF, are used as part of NSF's facility oversight and review process. This module will document NSF's expectation for the recipient and PO oversight for the implementation and monitoring of cyber-security best practices. These expectations extend over the full life cycle of an award, and are appropriately modified as the award passes through various stages of its life cycle.”

CTSC submitted a proposed version of the section to the Large Facilities Office.

For all Large Facilities to have **highly effective** cybersecurity programs.

In our experience, as both security practitioners and NSF community members, these are some of the features of security programs that inspire confidence.

1. A **budget** for both **personnel and tools**
2. Defined **governance** and **risk acceptance processes**
3. A **CISO** or similar role with **defined authority**
4. An **adopted framework** (e.g., CTSC's Guide, SANS Top 20, NIST Framework, NIST RMF, ISO)
5. Coordination of identity and access management (**IAM**).

New CCoE Activity: **Providing Situational Awareness**

Advise NSF LFs about **relevant software vulnerabilities** and provide guidance on mitigation.

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

Please subscribe to the email list(s) to receive situational awareness notifications of relevance to you.

Goal: 90% participation from LFs

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

IAM challenge for LFs: Enabling multi-organization, multi-national collaborations

CTSC IAM activities include:

- Engagements

- Sharing best practices and lessons learned

 - Blog posts, training, webinars

- Coordination with:

 - InCommon/Internet2

 - GÉANT/TERENA/REFEDS/AARC (EU Collaboration)

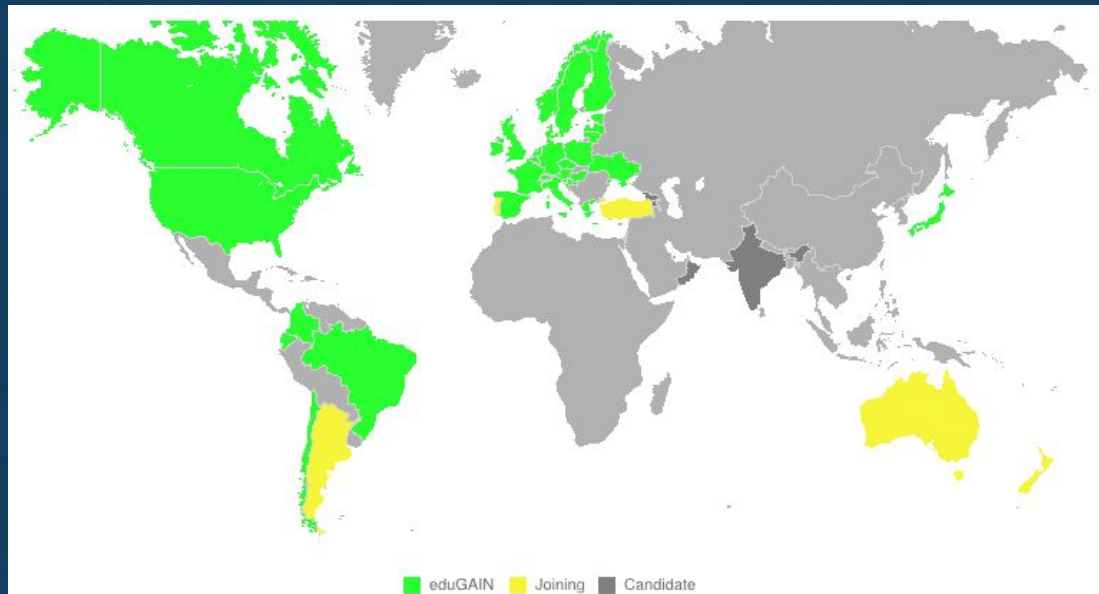
- Gathering community input (Summit, email lists)

trustedci.org/iam

InCommon went international in February!

CTSC & LIGO engagement launched InCommon's interederation working group in 2013.

blog.trustedci.org/2013/01/interfed.html



incommon.org/edugain/

How will CTSC help Large Facilities?

We know we're moving forward on these:

1. One on one engagements
2. Facilitating a community of practice around infosec
3. Organizing community activities and events (the Summit)
4. Training (like we've done with the Guide)
5. Better integrating IAM into our programmatic training
6. Developing a community survey
7. LF Manual Subsection
8. *Building on our reputation as a trusted partner and resource*

For all Large Facilities to have **highly effective** cybersecurity programs.

What would be helpful to CTSC's effort?

1. Contacts and connections with the facilities that are not engaged in events like the summit.
2. Support for Large Facility Community of Practice around information security.
3. Benchmarking data on cybersecurity (e.g., personnel budgets).
4. Feedback on Large Facilities challenges regarding information security.
5. Other suggestions, feedback, and comments are welcomed..

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
- Help to address the changing threat landscape for NSF CI

2015 Summit Highlights

*“Understanding the Information Assets
that Enable Science”*

- 90 Participants
- **Significant** growth in Call For Participation (17 submissions) had more proposals than available time
- Attendee evaluations and feedback were overwhelmingly positive - **95% rating summit as “good” or “excellent”**
- Expanded **training program to full day**

2016 Summit Call For Participation (CFP)

Now accepting community proposals:

- Plenary Presentations
- Training Sessions
- Table Talk Sessions
- Student Program
- CFP **Deadline June 3rd**

Seeking CFPs addressing:

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

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

More information: <http://trustedci.org/2016-nsf-cfp/>

2016 NSF Cybersecurity Summit:
August 16-18, 2016 - Arlington, Virginia

<http://trustedci.org/summit>



CENTER FOR TRUSTWORTHY
SCIENTIFIC CYBERINFRASTRUCTURE
The NSF Cybersecurity Center of Excellence

Thank You

trustedci.org

 [@TrustedCI](https://twitter.com/TrustedCI)

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.