Cybersecurity in the Cyberinfrastructure

2018 NSF Cybersecurity
August 22, 2018

Amy Friedlander

Deputy Office Director

Office of Advanced Cyberinfrastructure,

Directorate for Computer & Information Science & Engineering

National Science Foundation

Outline

NSF/OAC Update

OAC and Role of CI

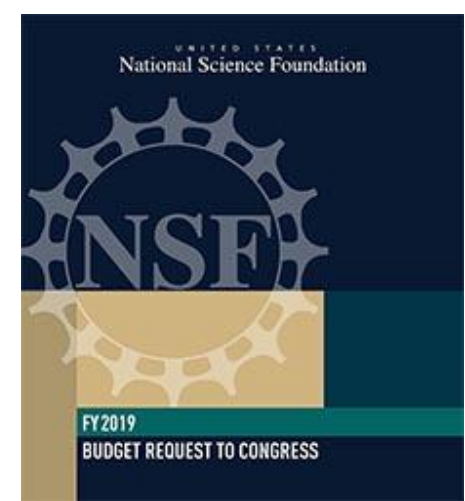Cybersecurity in the Cyberinfrastructure

What's next?

National Science Foundation's Mission

"To promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense…"

NSF Budget Update

FY 2018

- FY18 Congressionally Appropriated Budget
  - +4%
  - +$300M over FY17 budget!

- 2nd largest increase in NSF research budget increase in 15 years! (not counting ARRA)

FY 2019

- NSF: $7.47 billion
  - Flat with respect to FY 17 Enacted

- CISE: $925.4 million
  - -1.1% from FY 17 Enacted

- Big Ideas
  - Research Ideas: $30 million each
  - Process Ideas: Midscale infrastructure: $60 million

- Convergence Accelerators
  - $60 million
  - HDR, FW-HTF: $30 million each

The NSF Big Ideas

RESEARCH IDEAS

MATHEMATICAL, STATISTICAL, COMPUTATIONAL FOUNDATIONS
ANALYTICS DATA SCIENCE
HARNESSING THE DATA REVOLUTION
FUNDAMENTAL RESEARCH MACHINE DOMAIN SCIENCE RESEARCH LEARNING CHALLENGES DATA CYBERINFRASTRUCTURE MODELING DATA INTERNET OF THINGS STATISTICS MINING

Harnessing Data for 21st Century Science and Engineering

Work at the Human-Technology Frontier: Shaping the Future

Navigating the New Arctic

Windows on the Universe: Multi-messenger Astrophysics

Quantum Leap: Leading the Next Quantum Revolution

Understanding the Rules of Life: Predicting Phenotype

PROCESS IDEAS

Mid-scale Research Infrastructure

NSF 2026

Growing Convergence Research at NSF

NSF INCLUDES: Enhancing STEM through Diversity and Inclusion

" ... bold questions that will drive NSF's long-term research agenda -- questions that will ensure future generations continue to reap the benefits of fundamental S&E research. "

# Big Ideas => Big Cyberinfrastructure Challenges & Opportunities

Convergence Accelerators

Accelerating Discovery through Convergence Research

Motivation: Changing nature of science research - research frontiers at intersection of existing disciplines

- Time-limited entities: accelerating impactful *convergence* research in areas of national importance
- Innovating in organizational structure to better enable frontier research
- Separate (from directorates) in leadership, budget, and programmatics; but aligned with, relying on, and building on foundational disciplinary research
- Emphasis on translational research, partnerships

HDR Convergence Accelerator

FW-HTF Convergence Accelerator

Future accelerator(s)

BIO | CISE | EHR | ENG | GEO | MPS | SBE
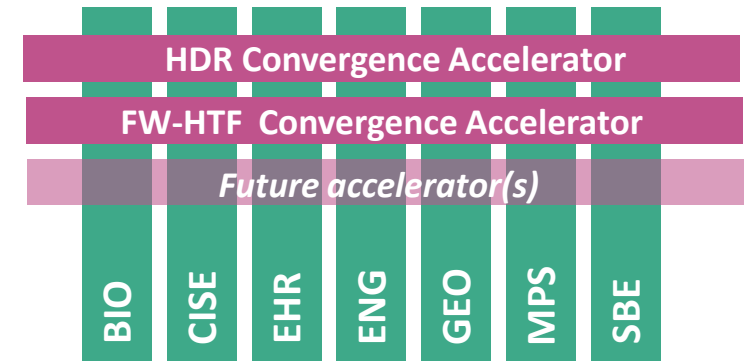
EXECUTIVE OFFICE OF THE PRESIDENT
WASHINGTON, D.C.

American Leadership in Artificial Intelligence, Quantum Information Sciences, and Strategic Computing

Continued leadership in AI, quantum information science (QIS), and strategic computing is critically important to our national security and economic competitiveness. Advances in these areas promise opportunities for major scientific breakthroughs and are quickly transforming American life and industry. Agencies should invest in fundamental and applied AI research, including machine learning, autonomous systems, and applications at the human-technology frontier. Agencies should prioritize QIS R&D, which will build the technical and scientific base necessary to explore the next generation of QIS theory, devices, and applications. Agencies should prioritize investment in research and infrastructure to maintain U.S. leadership in strategic computing, from edge devices to high-performance computing, that accelerates delivery of low-power, high performance devices; supports a national high-performance computing ecosystem; and explores novel pathways to advance computing in a post-Moore's Law era.

NSF Office of Advanced Cyberinfrastructure

Program Staff

Manish Parashar *
Office Director

Amy Friedlander
Deputy Office Director

Bill Miller
Science Advisor
(On Detail)

Computing	Data	Software	Networking & Cybersecurity	Learning & Workforce Development

Beth Plale *
Science Advisor
Public Access

Bob Chadduck

Amy Walton

Vipin Chaudhary *

TBD

Sushil Prasad *

Alejandro Suarez
Cooperative Agreements

Ed Walker

Stefan Robila *

Rajiv Ramnath *
(Part-Time)

Kevin Thompson

Scott Sellars
AAAS S&T Policy Fellow

Join NSF/OAC: Multiple Program Officer openings

August 22, 2018

* IPA Appointment

CISE/OAC – Transforming the Frontiers of Science & Society

Foster a cyberinfrastructure ecosystem to transform computational- and data-intensive research across all of science and engineering

- Cyberinfrastructure Research & Research Cyberinfrastructure
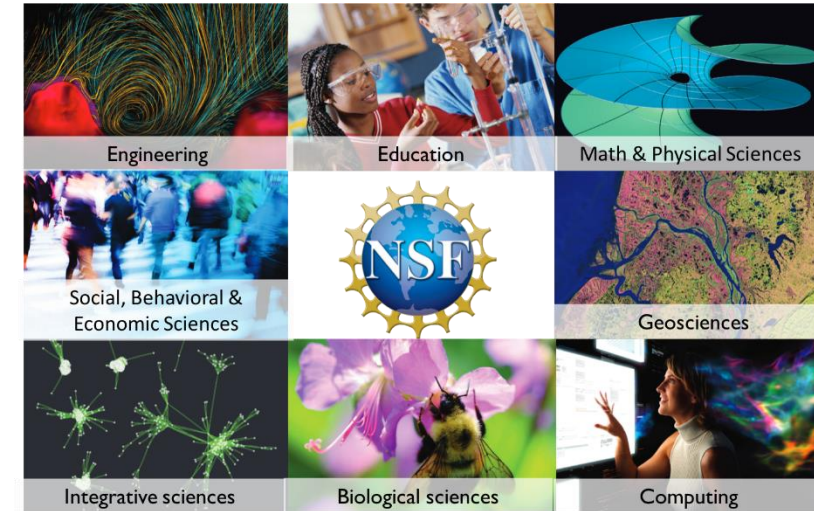
CI-Enabled Instrumentation

Computing Resources

Data Infrastructure

Gateways, Hubs, and Services

Cloud Resources & Services

R&E Networks, Security Layers

Coordination & User support

Software and Workflow Systems

Pilots, Testbeds

People, organizations, and communities

CISE/OAC – Transforming the Frontiers of Science & Society
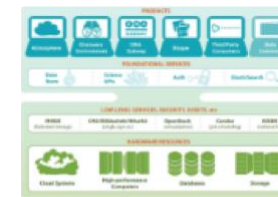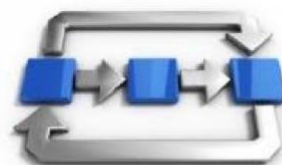
| Computing | Advanced resources and services at all scales – MRI (clusters); Innovative HPC; Leadership Class; XSEDE coordination and user services; Research |

Data — Data Building Blocks (DIBBS) Program

Software — Software Infrastructure for Sustained Innovation (SI2)

Cyberinfrastructure for Sustained Scientific Innovation (CSSI)

Networking & Cybersecurity — Campus Cyberinfrastructure (CC*), International Research Network Connections (IRNC), Cybersecurity Innovation for CI (CICI)

Learning & Workforce Devel — Training-based Workforce Development for Advanced Cyberinfrastructure (CyberTraining), CAREER, CRII

Emerging Opportunities — Cyberinfrastructure for Emerging Science and Engineering Research (CESER), Public Access

Large Facilities Present New Challenges, Opportunities

- Technology integration, capability evolution
- Integrated data lifecycle management
- Efficiencies, integration, interoperability across data/compute islands
- On-demand data processing, analytics, data product generation
- Enhanced (intelligent) data delivery
  - Open access, shared use, and beyond
- Data provenance, citation, reproducibility, …
- Cybersecurity
- …

NSF LARGE FACILITIES

CYBERINFRASTRUCTURE

Report from the NSF Large Facilities Cyberinfrastructure Workshop

Alexandria, VA, USA, September 6-7, 2017

August 22, 2018

11

http://www.facilitiesci.org/

Building on Community Input: Results of NSF CI 2030 Request for Information

Common needs expressed across science and engineering domains:

- **Advanced computing.** Growing need for <u>on-demand computing</u> for steering large simulations, rapid data processing, experiments; comparing simulations and observation.

- **Data Science and management.** <u>Big Data</u> and <u>Machine Learning</u>. Automated mining, analytics, visualization, provenance. Discoverability, accessibility, and reproducibility.

- **Multi-source streaming data**. Processing and integrating data from the <u>Internet of Things</u> (IOT) and cyber-physical systems at human, community, urban, and ecosystems scales.

- **Secure access, dynamic and high bandwidth workflows.** Technologies & approaches that scale with performance demands; storage, identity management, cybersecurity.

- **Software.** Porting, accelerating, validating algorithms and community codes. Software quality, reliability, validity, practices.

- **Training and workforce development.** For researchers and computing professionals, diversity and inclusion. CS/CI experts who collaborate closely with domain researchers.

All responses posted on CI 2030 Website: www.nsf.gov/cise/oac/ci2030/

NSF Workshop on Future Cyberinfrastructure: Rethinking NSF's Computational Ecosystem for 21st Century Science and Engineering (Alexandria, VA, May 30 - 31, 2018)

Early Recommendations / Emerging Strategic Directions:

- Delineate solicitations and investments in cyberinfrastructure innovation versus cyberinfrastructure operations, while recognizing the former ultimately informs the latter

- Consider a funding model that requires collaborations to drive interoperability and sustainability across scientific instruments and domains

- Explore new and creative kinds of partnerships – public-private and interagency – as necessary to sustain national research competitiveness and NSF leadership

- Develop a clear, long-term strategy, derived from principles that are clearly articulated and understood
    - Make difficult, strategic choices – rather than investing in too many things, should focus limited resources on those things only it can do best

Realizing a Cyberinfrastructure Ecosystem to Transform Science

■ Realize a holistic and integrated cyberinfrastructure ecosystem aimed at transforming science

■ Support the translational research continuum, from catalyzing core innovations, through fostering the community tools and frameworks, and enabling sustainable cyberinfrastructure services

■ Work closely with science and engineering communities, and other stakeholders to tightly couple the cycles of discovery and innovation

August 22, 2018

14
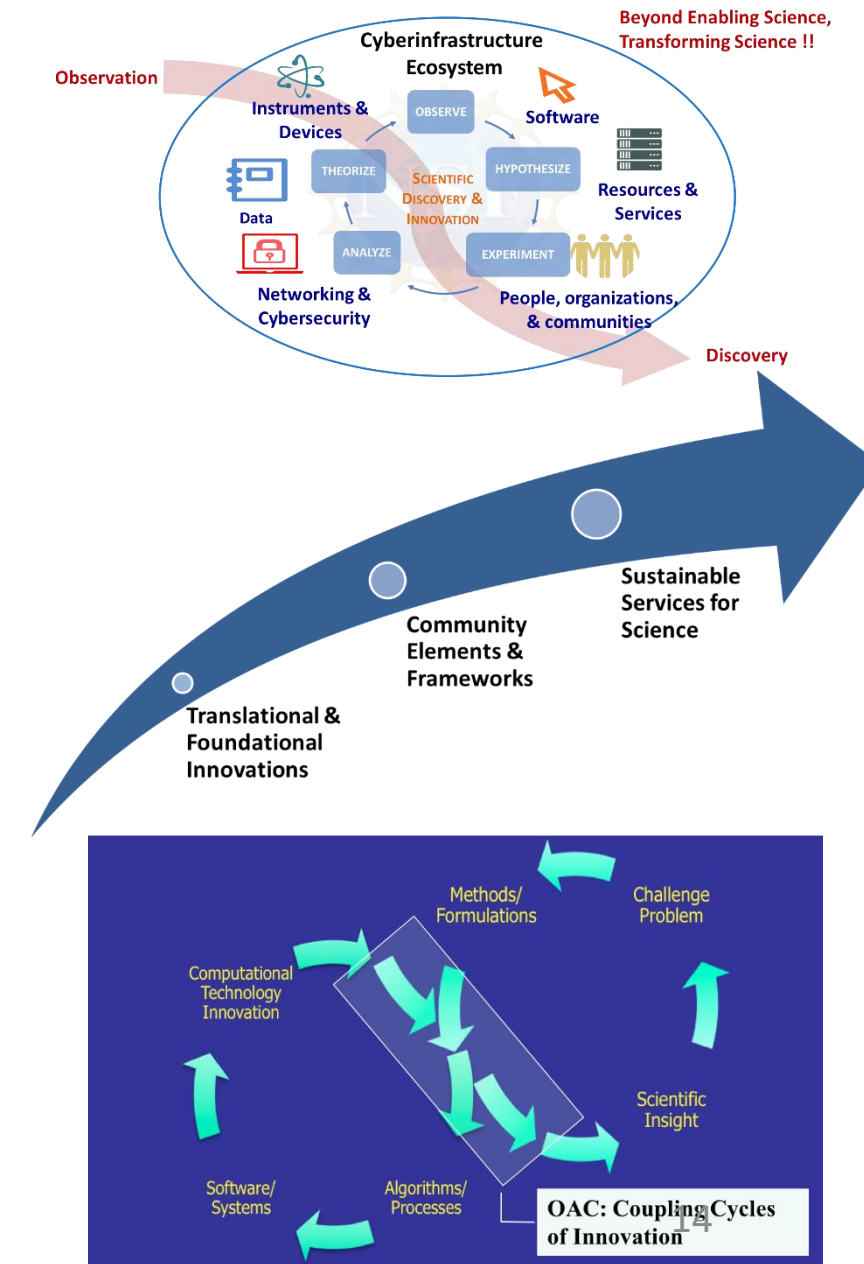
OAC Core Research Program

SOLICITATION NSF 18-567

- ***Translational research*** (spanning design to practice) in all aspects of advanced cyberinfrastructure (CI) to transform science and engineering research
  - Multi-disciplinary, extreme-scale, driven by science and engineering research, end-to-end, <u>or</u> deployable as robust research CI

- ***Research Areas***
  - *Architecture and middleware for extreme-scale systems*
  - *Scalable Algorithms and Applications*
  - *Advanced Cyberinfrastructure Ecosystem*

- ***Research Communities:*** Multiple disciplinary areas supported spanning Computer as well as Computational and Data-driven Science and Engineering

- Part of CISE's coordinated core program solicitations
  - Only Small proposals in FY'19
  - Funding amount $7.5M
  - Max $500K/award

- Proposals due Nov 15, 2018
  - PI's *strongly encouraged* to send 1-page project summary for further guidance.
  - Webinar in July/Aug

Cybersecurity is fundamental to the Research Scientific Environment

- Reproducibility
  - Integrity of data, software, and results
  - Embarrassment, damage to reputation, misinformation
- High value assets – understand and manage risk
- More instruments are network-connected
- Science is increasingly being conducted using non-traditional instruments: drones, sensors, smartphones, and so on

OAC Cybersecurity

- Scientific computing has distinctive security requirements.
- Cybersecurity portfolio consists of 2 types of awards:
  - Secure and Trustworthy Cyberspace (SaTC)
    - NSF's largest cross directorate program. Funds basic security and privacy research.
    - OAC focuses on Transition to Practice (TTP) projects, which aim to transition applied cybersecurity research projects into adoption and use in operational CI environments.
  - Cybersecurity Innovation for Cyberinfrastructure (CICI) program, which addresses the unique cybersecurity needs of CI in support of advanced computationally intensive scientific research.
- **Annual Large Facilities Cybersecurity Summit**. ~120 attendees from NSF-funded science facilities in 2017
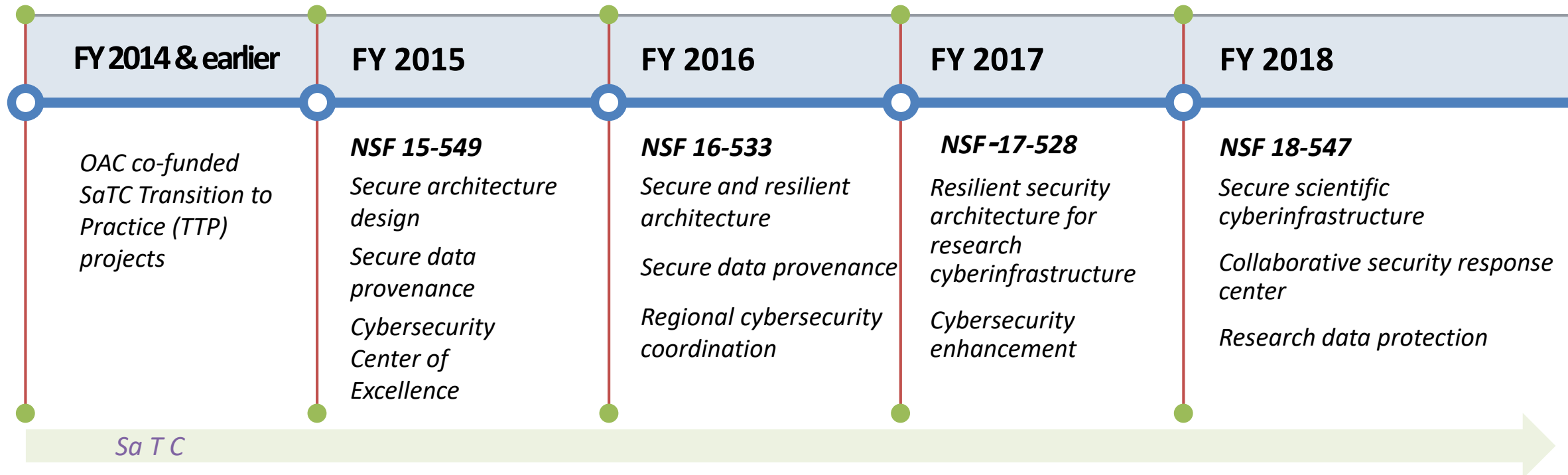
Example: Bro Intrusion Prevention/Detection software
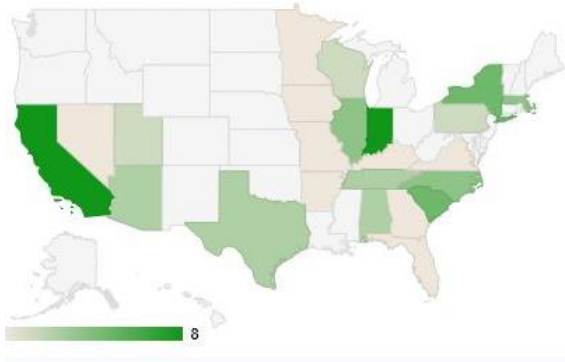
CICI was established in 2015 as a core program in CISE/OAC, offering new R&D opportunities impacting science environments .

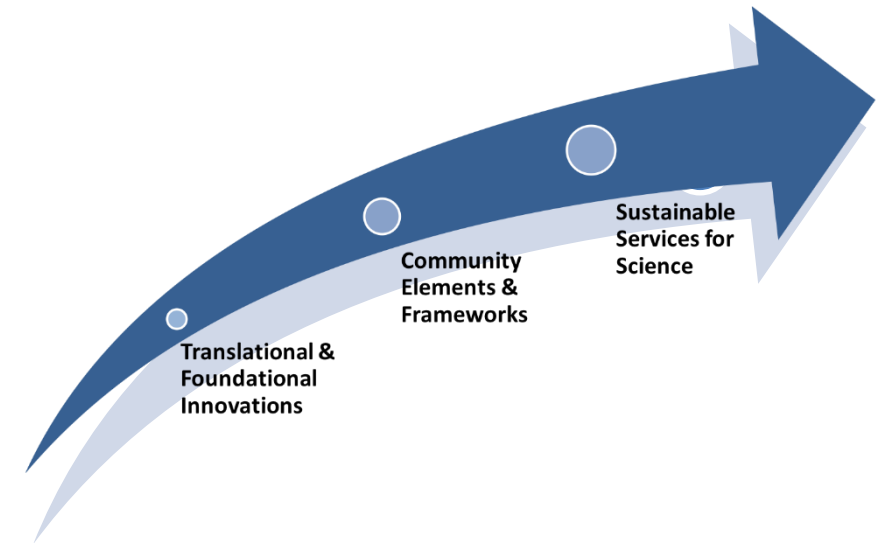| FY 2014 & earlier	FY 2015	FY 2016	FY 2017	FY 2018
OAC co-funded SaTC Transition to Practice (TTP) projects	**NSF 15-549** Secure architecture design Secure data provenance Cybersecurity Center of Excellence	**NSF 16-533** Secure and resilient architecture Secure data provenance Regional cybersecurity coordination	**NSF-17-528** Resilient security architecture for research cyberinfrastructure Cybersecurity enhancement	**NSF 18-547** Secure scientific cyberinfrastructure Collaborative security response center Research data protection

Sa T C

CICI: Observations

Areas of Interest

- Secure interoperability of cloud/campus/facility
- Security Metrics; data analytics; trend analysis methodologies
- Distributed Denial of Service (DDoS) Defense
- New approaches to securing key infrastructure
- Identity and Attribute management
- Data integrity techniques
- Techniques and tools to detect behavioral anomalies
- Secure emerging technologies such as Software Defined Networking (SDN)
- Define organizational risk management posture
- Regional cooperation for cybersecurity
- Building centralized knowledge and services (CCoE and CSRC)

Trends

- Augmented interest beyond architecture/ networking
- Integration with data

Sustainable Services for Science

Community Elements & Frameworks

Translational & Foundational Innovations

Conclusion

- Science and society are being transformed by compute and data – an integrated cyberinfrastructure ecosystem is essential

- Rapidly changing application requirements; resource and technology landscapes
  - Our cyberinfrastructure ecosystem must evolve in response
  - ***And it must be secure, reliable, and trustworthy***

- Lets build a holistic and integrated cyberinfrastructure ecosystem aimed at transforming science

Join the conversation

- OAC Webinar Series
  - 3rd Thursday @ 2PM ET
- OAC Newsletter
- Follow us on Twitter @NSF_CISE

Stay informed

- Join the OAC, CISE Mailing Lists

  - Learn about NSF events, programs, webinars, etc.

  - Send email to:

    - oac-announce@listserv.nsf.gov

    - cise-announce-subscribe-request@listserv.nsf.gov

Get involved

- Reviews proposals, serve on panels
- Visit NSF, get to know your programs and Program Officers
- Participate in NSF workshops and visioning activities
- Join NSF: serve as Program Officer, Division Director, or Science Advisor

NSF Office of Advanced Cyberinfrastructure (OAC) Newsletter

Table of Contents

- About the Office
- Project Highlights
- OAC Program and Updates
- Related Events/Programs
- Subscribe to OAC Mailing List

TWEETS 1,075   FOLLOWING 27   FOLLOWERS 2,050   Following

NSF Comp & Info
@NSF_CISE

Exploring the frontiers of computing

Arlington, Virginia · nsf.gov/dir/index.jsp?...

"Make no little plans; They have no magic to stir men's blood ..."

Daniel H. Burnham, Architect and City Planner Extraordinaire, 1907.

"If you want to travel fast, travel alone;
if you want to travel far, travel together"

African Proverb.

THANKS!

Amy Friedlander

Deputy Office Director, Office of Advanced Cyberinfrastructure

Email: afriedla@nsf.gov

To subscribe to the OAC Announce Mailing List
Send an email to: OAC-ANNOUNCE-subscribe-request@listserv.nsf.gov

August 22, 2018

22