NSF Cyberinfrastructure Cybersecurity: Research Challenges to Production Capabilities

Research Infrastructure Workshop

Washington, DC

June 28, 2023

Robert Beverly

National Science Foundation

Office of Advanced Cyberinfrastructure

NSF's CISE/OAC and Scientific Cyberinfrastructure

- **Office of Advanced Cyberinfrastructure**: Supports and coordinates the development, acquisition and provisioning of state-of-the-art cyberinfrastructure resources, tools and services essential to the advancement and transformation of science and engineering.

- **Cyberinfrastructure (CI)**: Compute, data, software, networking, and people to facilitate scientific discovery and innovation.

NSF Office of Advanced Cyberinfrastructure (OAC)

Foster a cyberinfrastructure (CI) ecosystem to transform science and engineering research… through Research CI and CI research

Observation

This Talk

People, organizations, and communities

Coordination & User support

Gateways, Hubs, and Services

Data Infrastructure

Software and Workflow Systems

CI-Enabled Instrumentation

Pilots, Testbeds

Discovery

Computing Resources

R&E Networks, Security Layers

Cloud Resources & Services

NSF's CISE/OAC and Scientific Cyberinfrastructure

- **Office of Advanced Cyberinfrastructure**: Supports and coordinates the development, acquisition and provisioning of state-of-the-art cyberinfrastructure resources, tools and services ess and eng

Cannot realize science goals unless cyberinfrastructure is secure, robust, and trustworthy.

- **Cyberinfrastructure (CI)**: Compute, data, software, networking and people to facilitate scientific discovery and innovation.

Cannot realize science goals unless cyberinfrastructure is secure, robust, and trustworthy

- Remainder of this talk:
  - What does it mean to “secure” science CI?
  - What is the role of cybersecurity in large CI and facilities?
  - Strategic efforts in supporting CI cybersecurity
  - Receive feedback from community

Cyberinfrastructure Challenges at Large Facilities

- **Bespoke environments** with
- **Large instruments** producing
- **Big data** requiring
- **Big compute** for
- **Collaborative** science in
- **Different specializations** across
- **Widely Distributed infrastructure** that must be
- **Available**, ensure
- **rity**, and be
- ile adhering to
- olicy
- requirements

CI Cybersecurity: An Enabler of Open and Collaborative Science

The Unique Research Cyberinfrastructure Ecosystem

	MISSION		HARDWARE		APPLICATIONS	
ENTERPRISE:						
SCIENCE CI:						
	PHYSICAL ENVIRONMENT		OPERATING SYSTEM			RISK

Whither Cybersecurity: We do open and unclassified science!”

- How can cybersecurity benefit the cyberinfrastructure?
- Imagine a world where…
  - Data has strong integrity protection, to prevent accidental or malicious modification
  - Research artifacts contain provenance meta-data
  - Collaboration between scientists and infrastructure is seamless and natural
  - Computation on, and sharing of, sensitive data is possible without compromising privacy
  - Infrastructure is highly available and not vulnerable to mis-use
  - Third-parties can replicate and reproduce research findings
  - The public trusts science

2022: White House Office of Science and Technology (OSTP) guidance on Open Science and Public Access

Issued by OSTP
Acting Director Alondra Nelson

- calls for **Free**, **Immediate**, and **Equitable** public access
- new Public Acc
  2023 (with pol
  by 2025)
- default **zero-embargo** of peer-reviewed articles and underlying data

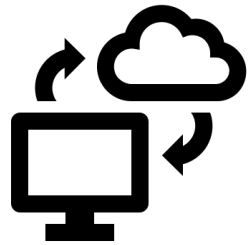
"For the purposes of this memorandum, 'scientific data' include the recorded factual material commonly accepted
in the scientific community as of sufficient quality to validate and replicate research findings."

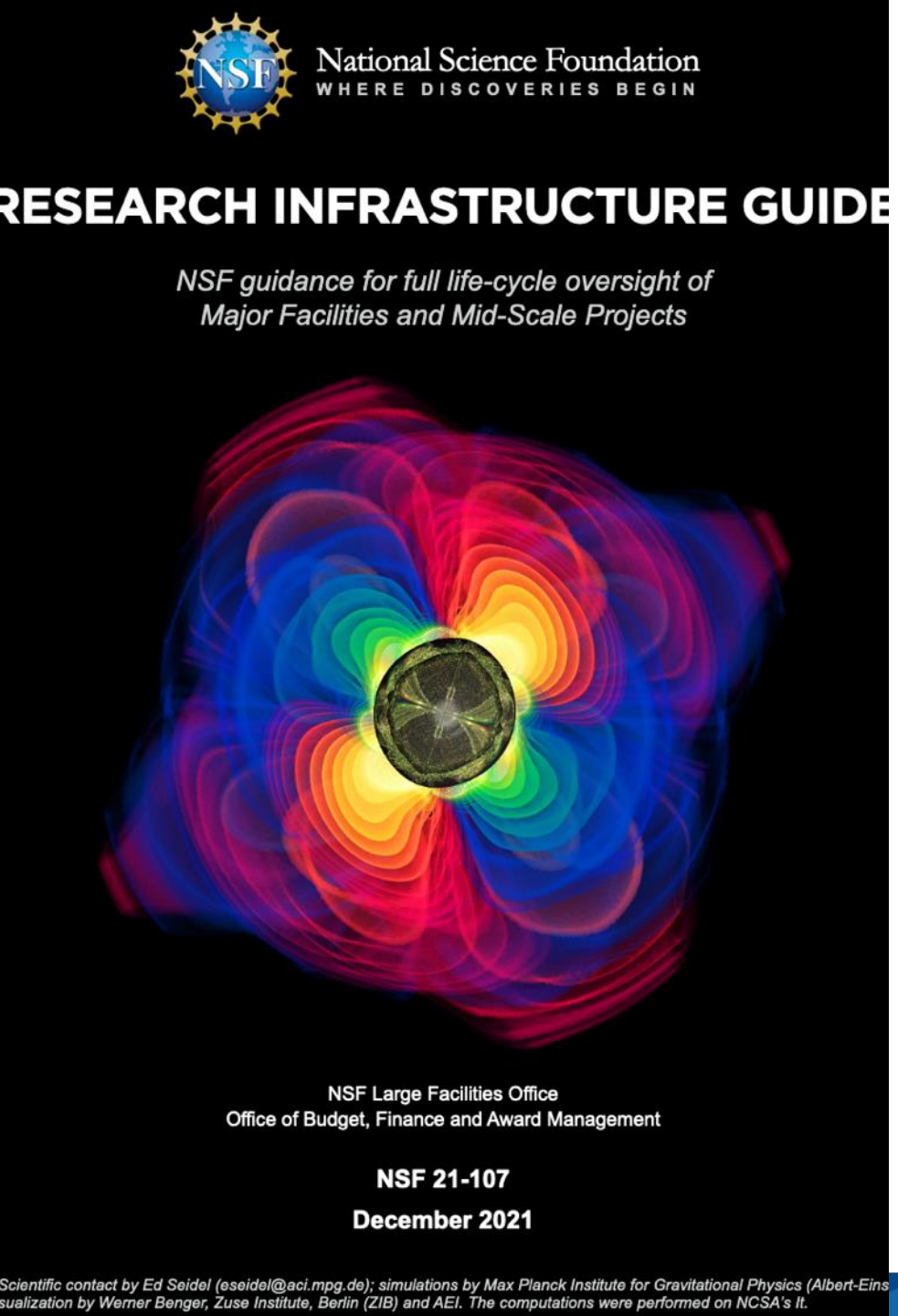
NSF Public Access Plan 2.0: NSF 23-104


EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C. 20502

August 25, 2022

CI Cybersecurity Benefits Across Organization

SCIENTIST	COLLEAGUE	MANAGEMENT	RESEARCH OFFICE	INFO TECH	PUBLIC
					
• Do research!	• Share Data + resources • Reproducibility • Integrity	• Reputation • Finance	• Protect IP	• Availability	• Trust in science



Cybersecurity@Facilities: The Why

- "Data creation, sharing, and analysis are central to the progress of science"
- "Cybersecurity protects the availability of instruments and systems; promotes trust in, and availability of, data; and provides confidence in the integrity of the research resulting from use of facility information"
- "Inappropriate, inefficient, and ineffective cybersecurity can be costly in time, human capital, and funding"

RIG Cybersecurity: Inspired by Trusted CI Framework

- Focus on mission-oriented cybersecurity, not compliance
- Ongoing and evolving
- Full scope of cybersecurity decision making

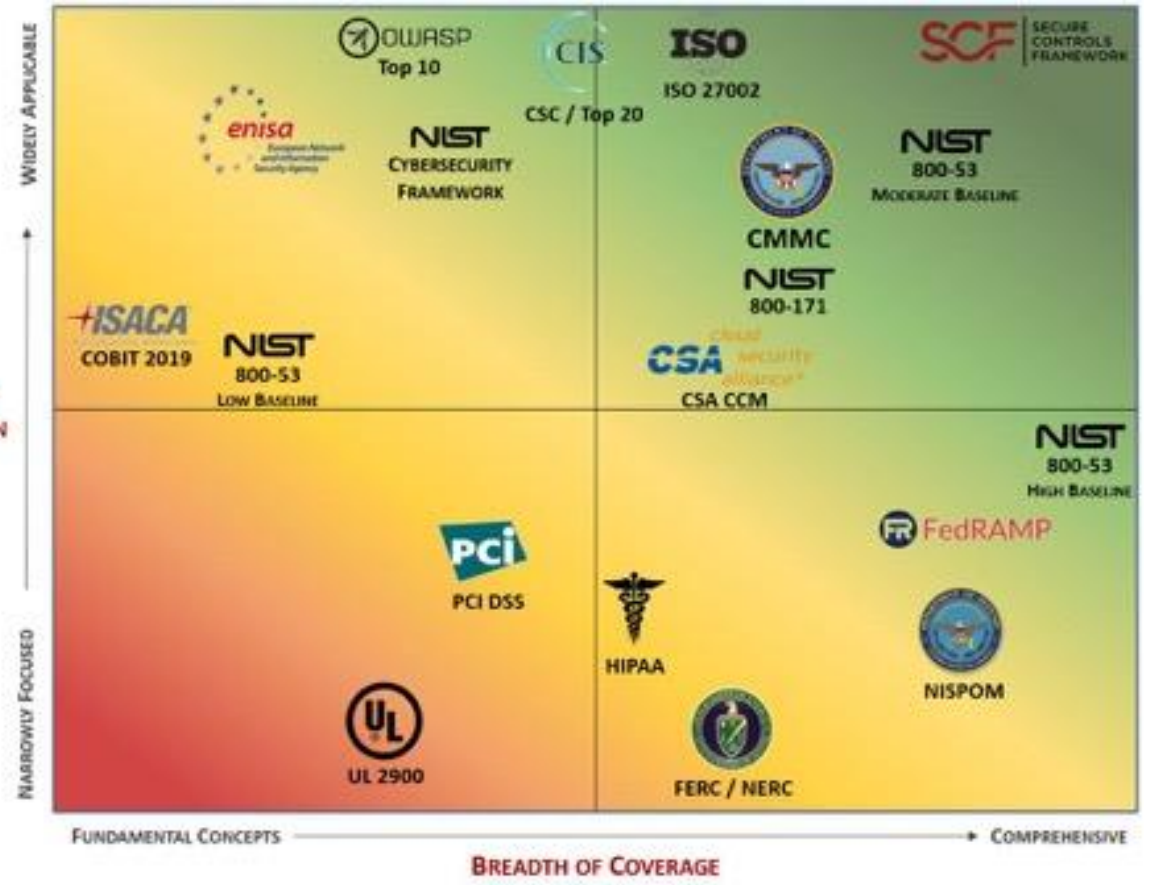
- Pillars:
  - Governance
  - Resources
  - Controls
  - Mission Alignment

RIG Cybersecurity Thematics

- Explicit acknowledgement of individual facility uniqueness and requirements:
  - “The foundation for developing and maintaining a project’s cybersecurity program lies in the research mission and goals of the facility itself”
- Incentivize cybersecurity rather than mandate / regulate / audit
  - Carrots vs. sticks: provide supporting resources that benefit cyberinfrastructure, facility, and scientific discovery mission
- Living document:
  - As cybersecurity techniques, tools, and threats evolve, so too do the guidelines

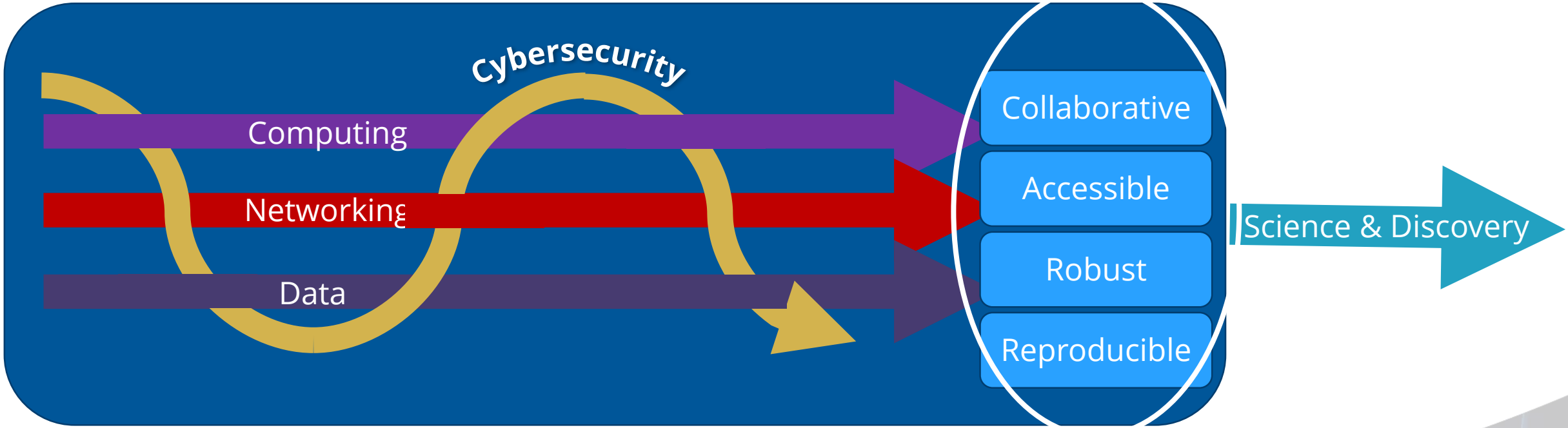
Carrots vs. Sticks

- NSF facilities, projects, and CI have a responsibility to protect public investments
  - But, also, unique mission for open science to advance discovery
  - Many cybersecurity frameworks overly onerous and/or not aligned with facility mission
- Instead, NSF OAC is supporting:
  - Platforms
  - Technologies
  - Proactive Defenses
  - Engagements

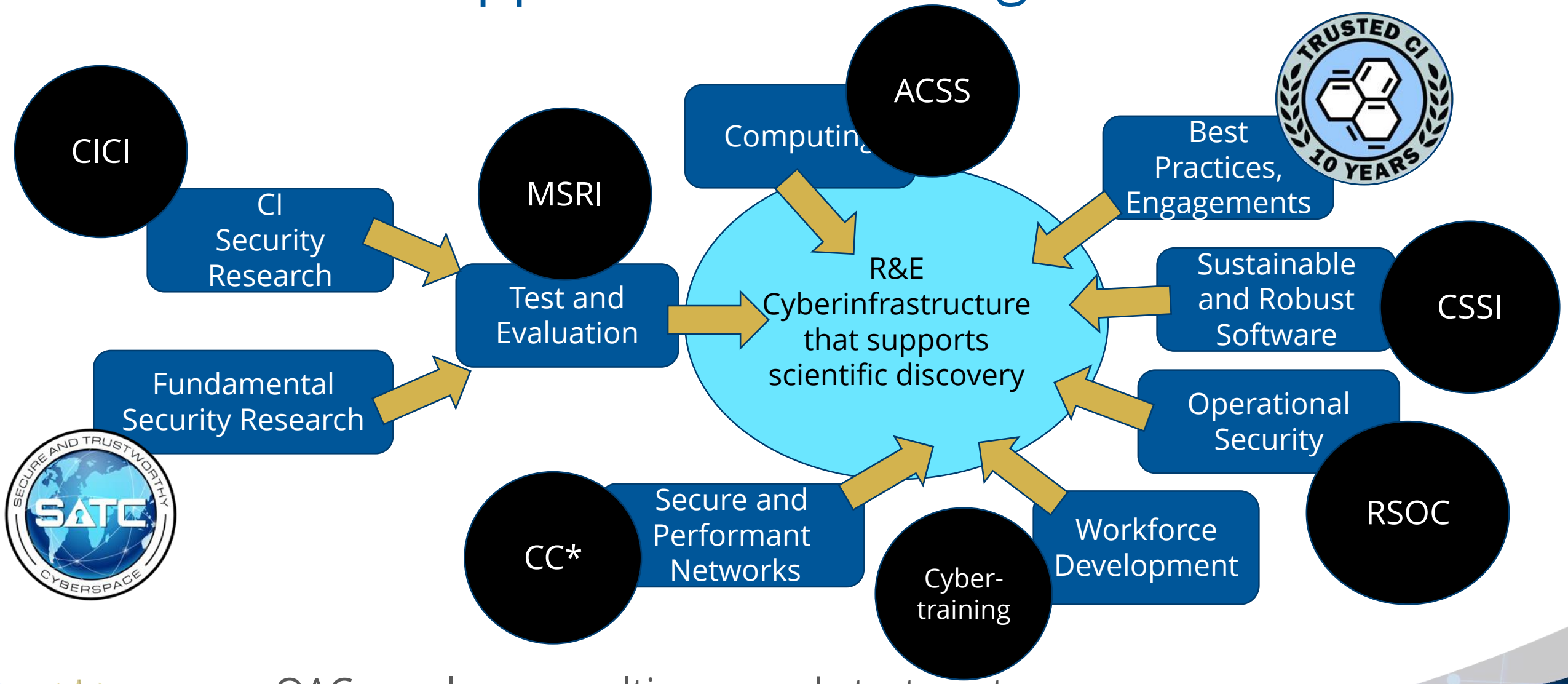


OAC CI Cybersecurity Vision

NSF's Blueprint for a National CI Ecosystem for the 21st Century: *"Agile, integrated, **robust**, **trustworthy**, and sustainable CI ecosystem that drives new thinking and transformative discoveries in all areas of S&E research and education"*



Holistic Approach to Securing CI



OAC employs a multi-pronged strategy to ensure security supports the scientific discovery mission

Cybersecurity Innovation for Cyberinfrastructure (CICI)

To advance science and discovery, supporting cyberinfrastructure must be *robust, trustworthy, collaborative, and compliant.* CICI:

- Operationalize emerging security into research CI
- Develop new security techniques specific to CI
- Transition for cyberresilience

collaboration

reproducibility

production

Example Projects

- ***Cyber Reasoning System**: Scientific Binary vuln detection and auto patching (ASU)*
- ***ARMOR**: Computing / search on encrypted data in HPC* (Augusta)
- ***SciAuth**: Deploying Interoperable and Usable Authorization Tokens* (UIUC)
- *Vulnerability Detection in **Configurable** Scientific Computing* (Utah)
- ***Open Science Chain** for Protecting Integrity and Provenance of Research Data* (UCSD)

Community Support:

- ***TrustedCI CoE***: Cybersec engagements with NSF projects and facilities
- ***ResearchSOC***: Operational cybersecurity protection and 24/7 monitoring
- ***RRCoP**: Regulated research community of practice*

2023 NSF Cybersecurity Summit

NSF Cyberinfrastructure Cybersecurity Summit

- Hosted by Trusted CI
- Berkeley, CA: October 24-26, 2023
- https://www.trustedci.org/2023-cybersecurity-summit

JASON Report on Facilities Cybersecurity

Recommendation: An executive position for cybersecurity strategy and coordination for major facilities should be created at NSF. This executive should have authorities that allow them to continually support the balancing of cybersecurity, scientific progress, and cost in the distinct ways that will be appropriate for each facility.

Mike Corn

Thank You

"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.

More info: https://www.nsf.gov/div/index.jsp?div=OAC

We want your input:

What is OAC doing right?

What could OAC do better?

What should OAC be doing?

Anytime: rbeverly@nsf.gov

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

20