TRUSTED CI

THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

trustedci.org

Trusted CI Framework for Open Science Cybersecurity Programs

Bob Cowles

SIG-ISM / WISE Meeting
Kaunas, Lithuania
April 17, 2019

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Trusted CI:
The NSF Cybersecurity Center of Excellence

Our mission: to 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.

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

NCSA

INTERNET2®

WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

PITTSBURGH SUPERCOMPUTING CENTER

BERKELEY LAB

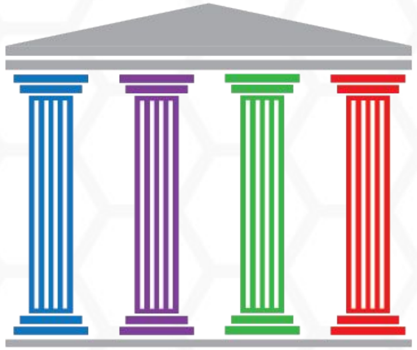
TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

https://trustedci.org/

The Concern

1. There is pressure on U.S. education and research to adopt NIST SP 800-171 (Controlled Unclassified Information) & other cybersecurity control frameworks.
2. These frameworks are not the most appropriate for open science where integrity and availability are as important, if not more so, than confidentiality.
3. Even if we accept 800-171 today, we “cede the ground” and may find those programs changed in the future.

Our Path Forward



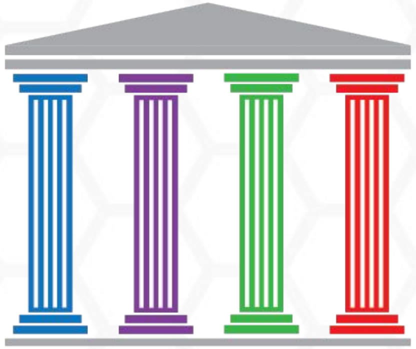
Build on the Trusted CI *Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects*

https://trustedci.org/guide

Create for Open Science a Trusted CI Framework with Framework Implementation Guides (FIGs).

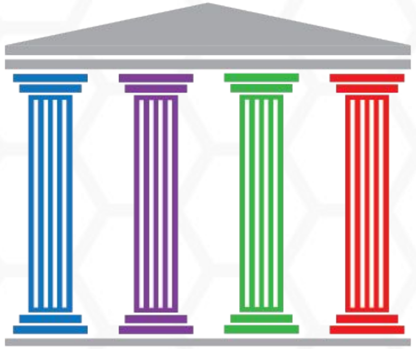
It is a multi-year effort with early adopters and quick wins needed for success.

Framework Goals



- Describe appropriate cybersecurity programs for both open science infrastructures and projects - even those using NIST control sets.
- Develop an initial FIG oriented toward research centers and medium-to-large science infrastructure projects.
- Be accepted by NSF, CIOs, CISOs, Projects Leads as an acceptable cybersecurity program.
- Stretch goal: Be accepted by an external-to-higher-education auditor or prime contractor.

The Trusted CI Framework



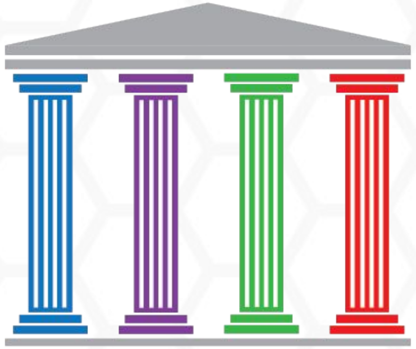
Framework Foundation:

- Concise, clear minimum requirements for cybersecurity programs organized under the 4 Pillars: Mission Alignment, Governance, Resources, and Controls
- Based on cybersecurity best practices and evidence of what works.
- Infrequent updates.

Framework Implementation Guides (FIGs):

- Guidance vetted by and tailored to the open science community.
- Curated pointers to the very best resources and tools.
- Frequent (at least yearly) updates.

Framework Pillars



Mission Alignment

- Information classification, asset inventory, external requirements

Governance

- Roles and responsibilities, policies, risk acceptance, program evaluation

Resources

- People, budgets, services and tools

Controls

- Procedural, technical, administrative safeguards and countermeasures

Framework Musts (Mission Alignment)

- Organizations must establish and maintain a **cybersecurity program** tailored to the organization's **mission**.
- Organizations must identify and account for **cybersecurity stakeholders** and **requirements**.
- Organizations must establish and maintain an **inventory** of **information assets**.
- Organizations must establish and implement a **structure for classifying** information assets as they relate to the organization's mission.

Framework Musts (Governance)

- Organizations must involve **leadership** in cybersecurity decision making.
- Organizations must formalize roles and responsibilities for cybersecurity **risk acceptance**.
- Organizations must establish a **lead role** with responsibility to advise and provide services to the organization on cybersecurity matters.
- Organizations must ensure the cybersecurity program **extends to all entities** with access to, control over, or authority over information assets.
- Organizations must develop, adopt, explain, follow, enforce, and revise cybersecurity **policy**.
- Organizations must **evaluate** and refine their cybersecurity program.

Framework Musts (Resources)

- Organizations must devote **adequate resources** to mitigate cybersecurity risks deemed unacceptable by the organization.
- Organizations must establish and maintain a cybersecurity **budget**.
- Organizations must allocate **personnel** resources to cybersecurity.
- Organizations must identify **external cybersecurity resources** to support the cybersecurity program.

Framework Musts (Controls)

- Organizations must adopt and utilize a **baseline control set**.
- Organizations must select and deploy **additional and alternate controls** as warranted.

Model "Must" Description

4.1 Organizations must adopt and utilize a baseline control set.

A baseline control set is a predetermined set of security controls used as a default when selecting security controls for information assets. The control set does not determine what security controls an organization **must** select; rather, it provides a foundation from which an organization tailors control selection based on the needs of its mission. Baseline control sets vary in the number, specificity, and goals of the controls they prescribe. For instance, baseline control sets may be legally imposed when handling specific types of data. In other cases, organizations can select one of the widely used evidenced-based control sets.

FIG Section Outline

In addition to the description (What) for each Must, the FIG will answer the following questions:

- Why - motivation
- Who - responsible entities
- How - implementation guidance
- When - sequencing considerations

Acknowledgments

Trusted CI is supported by the National Science Foundation under Grant ACI-1547272. The views expressed do not necessarily reflect the views of the National Science Foundation or any other organization.

Trusted CI activities are made possible thanks to the contributions of a multi-institutional team:

https://trustedci.org/who-we-are/

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Questions for Discussion (now and later)

- Do we have the challenges and goals right?
- What would you like to see in the Framework?
- What attributes do you think the Framework must have?
- What do you think the Framework must avoid?
- What other advice would you give us?
- Can we develop a statement of collaboration? (and add Trusted CI to Jim Marsteller's name on steering committee?)