The Trusted CI Framework for Cybersecurity Programs

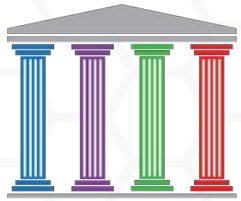
MS-CC All Hands Meeting

Jim Basney
Principal Research Scientist, Cybersecurity, NCSA, UIUC
Director and PI, Trusted CI
jbasney@ncsa.illinois.edu

August 24, 2023

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Outline



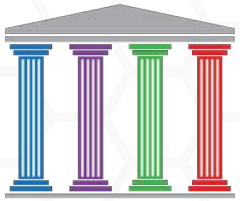
1. Trusted CI: Introduction
2. Trusted CI Framework for cybersecurity programs
3. What is a cybersecurity program?
4. Adopting the Trusted CI Framework
5. Highlights of the Trusted CI Framework

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Trusted CI

An Introduction

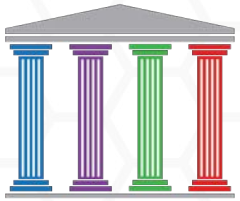
Trusted CI: An Introduction



1. Trusted CI is the NSF Cybersecurity Center of Excellence
   - Established in 2012
   - Collaboration between IU, UIUC, PSC, LBL, USA, and UW:M.
   - Currently on a 5 year cooperative agreement with the NSF
   - We work with the NSF community to improve the cybersecurity of cyberinfrastructure
2. **Our goal**: Help NSF cyberinfrastructure operators build effective cybersecurity programs
   - Assessments, trainings, consultations, cohorts, recommendations, community events, etc.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Community Resources



Ransomware
https://www.trustedci.org/ransomware

Research Transition to Practice
https://www.trustedci.org/ttp

Identity and Access Management
https://www.trustedci.org/iam

Software Assurance
https://www.trustedci.org/software-assurance

Operational Technology
https://www.trustedci.org/operational-technology

Science DMZs
https://www.trustedci.org/science-dmz

Trustworthy Data
https://www.trustedci.org/trustworthy-data

Compliance Programs
https://www.trustedci.org/compliance-programs

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

September 14-15 TTP Workshop

Virtual workshop on cybersecurity research transition to practice (TTP)

Registration now open

https://www.trustedci.org/ttp

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

NSF Cybersecurity Summit

Hybrid meeting
Registration now open

October 23-26, 2023 at
Lawrence Berkeley National
Laboratory in Berkeley, CA

https://trustedci.org/summit/

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

DAY 1 Monday October 23, 2023 | Workshops/Trainings

	Track 1	Track 2	Track 3	Track 4
8:00AM	*Sign-In and Continental Breakfast*			
9:00AM–1:00PM (Refreshment break at 10:30)	Zeek Training: Hands-on Zeek Scripting	Zeek Training: Intermediate to Zeek	Jupyter Security Workshop	
1:00–2:00PM	*Lunch*			
2:00 PM–5:00 PM (Refreshment break at 3:30)	Zeek Training: Hands-on Zeek Scripting	Zeek Training: Intermediate to Zeek	Jupyter Security Workshop	WISE Community Workshop

DAY 2 Tuesday October 24, 2023 | Plenary and Workshops/Trainings

7:00 AM	*Sign-In and Continental Breakfast*		
8:00 AM	*Welcome & NSF Address*		
8:30 AM	*Berkeley Welcome & ESNet Welcome*		
9:00 AM	*Trusted CI Update*		
9:30 AM	*Keynote #1 (TBA)*		
10:00 AM	*Keynote #2 (TBA)*		
10:30 AM	*Refreshment Break*		
11:00 AM	*Plenary Session	Implementing NIST 800-171 in a both distributed and centralized environment*		
11:30 AM	*Plenary Session	Unmasking Shadows: Investigating MICI-BICA, an Incident Involving IRC-Based Malware Deployment, Rootkit Stealth, and Self-Hiding Cryptominers*		
12:00 PM	*Plenary Session	Black Hole Locker Ransomware : Affiliate program*		
12:30–2:00 PM	*Lunch*			
	Track 1	Track 2	Track 3
2:00–5:00 PM (coffee break at 3:30)	*Securing your Code with Better Coding Practices and Tools*	*Jupyter Network Monitoring with Zeek Workshop*	*Security intrusion at the Zebra Scientific Alliance*
5:30-7:30 PM	**Social night -Residence Inn Study hall rooftop**-2121 Center St, Berkeley,		

DAY 3 | Wednesday October 25, 2023 | Plenary and Workshops/Trainings /BoFs/Project Mtgs

7:00 AM	*Sign-In and Continental Breakfast*			
8:00 AM	*Plenary Session	Principles of Decentralized Cyberinfrastructure*			
8:30 AM	*Plenary Session 5	(TBA)*			
9:00 AM	*Plenary Session 6	(TBA)*			
	Track 1	Track 2	Track 3	Track 4/Project Meetings
9:30 am–12:30 PM (coffee break at 10:30)	Deep Machine Learning for Intrusion Detection in Cyber-Physical Critical Infrastructures	Physical Security is Important Um'k	Regulatory Compliance for Research: DFARS/CMMC, HIPAA, GDPR, NSPM-33	SAFER Member Meeting (Members Only)
12:30–2:00 PM	*Lunch*			
2:00 PM	Catch Me If You GPT: Tutorial on Deepfake Texts	BOF: Research Security Compliance collaborations to support PI research	The Trusted CI Framework: Strategies for Getting Started	ACCESS CONECT Cybersecurity Group and invited guests. 20 people (2:00-4:00 PM)
3:30 PM	*Refreshment Break*			
4:00 PM	Catch Me If You GPT: Tutorial on Deepfake Texts	BoF: NICE Workforce Framework Adoption: Cybersecurity Teaching Innovations	The Trusted CI Framework: Strategies for Getting Started	SAFER Member Meeting CONTINUED (Members Only)
5:00 PM	*Conclude*			

DAY 4 | Thursday October 26 - Plenary and Workshops/Trainings/BoFs

7:00 AM	*Sign-In and Continental Breakfast*		
	Track 1	Track 2	Track 3
8:00 AM	[TLP:RED] How we failed to handle a triple-combo attack against the R&E HPC community worldwide...in the middle of a pandemic	Trusted CI Framework Community of Practice (CoP) Quarterly Meeting (8:00 – 11:00 AM)	Security Log Analysis (8:00 – 11:00 AM)
8:30 AM	[TLP:RED] Monero mining, with love, from space		
9:00 AM	[TLP:RED] Reserved		
9:30 AM	[TLP:RED] Reserved		
10:00 AM	[TLP:RED] Reserved		
10:30 AM	pDNSSOC: Correlating DNS logs with threat intel from MISP as a poor man's SOC. (10:30-12:00 PM)		
11:00 AM	Experiences from SIO (CCRV) and OSU (RCRVs) in Cybersecure-by-Design Ship Design and Construction (11:00 AM-12:00 PM)		
12:00-1:30 PM	*Lunch*		
1:30 PM	**Plenary Session	US Academic Research Fleet (ARF) Cyber Risk Management Program (CRMP)**		
2:00 PM	**Plenary Session	Cyber Forensics In Everyday Business**		
2:30 PM	***Poster Session / Ice Cream Break /Refreshment***		
3:30 PM	***Plenary Session	Trusted CI Fellows Panel***		
4:00 PM	***Plenary Session	(TBA)***		
4:30 PM	***Summit Observations and feedback***		
5:00 PM	***Adjourn***		

Monthly Webinars

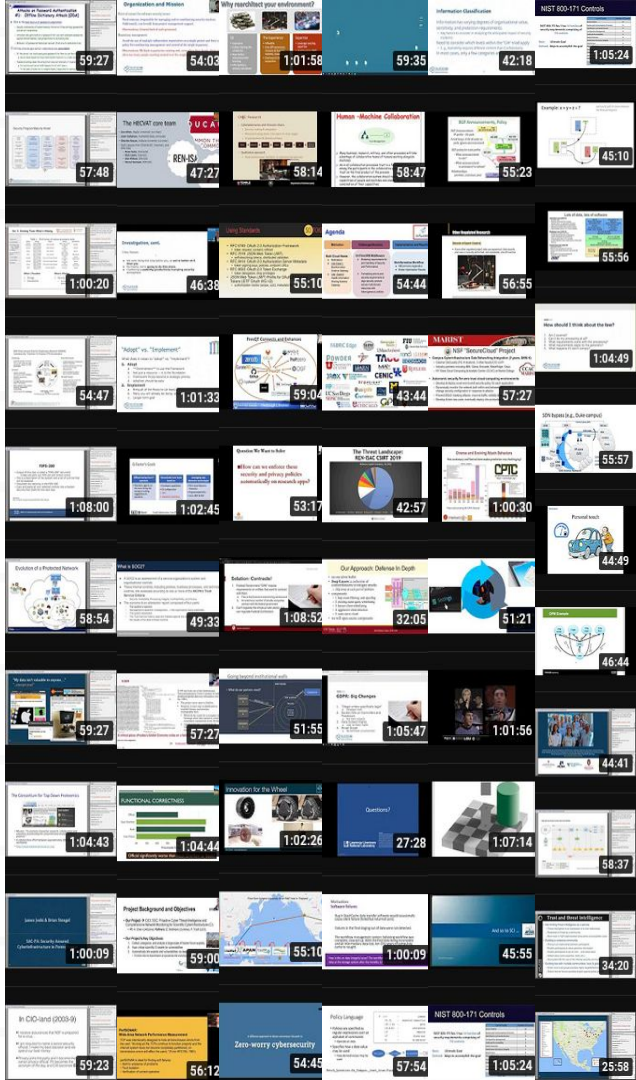
Cybersecurity for Cyberinfrastructure

Community presentations about cybersecurity research results, operational practices, lessons learned, etc.

4th Monday of the month at 11am Eastern

https://www.trustedci.org/webinars

https://www.trustedci.org/trustedci-email-lists



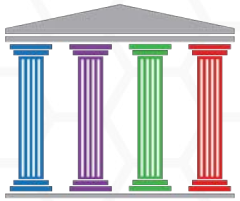
TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

The Trusted CI Framework

An Overview

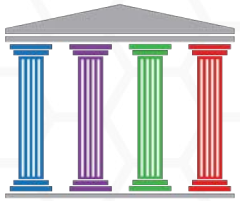
TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Cybersecurity Programs



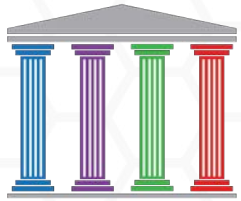
1. We regularly conduct assessments, trainings, consultations, and other types of engagements with a wide range of organizations.
2. The primary challenges organizations face with cybersecurity are not technical: They are on programmatic elements.
   a. Money
   b. Governance
   c. Leadership Involvement
   d. Mission Alignment
3. Organizations lack guidance on how to address these non-technical elements

Cybersecurity Programs



1. Many organizations anticipate incoming cybersecurity compliance
    a. Controlled Unclassified Information & NIST SP 800-171
    b. Cybersecurity Maturity Model Certification
    c. National Security Presidential Memorandum 33
    d. FISMA
2. These compliance control sets typically focus on technology, and don't address those key enablers of cybersecurity.
3. Without a cybersecurity program, organizations often don't even know where to begin when handed a cybersecurity control set.

The Trusted CI Framework



The Trusted CI Framework establishes a **minimum standard** for cybersecurity programs.

- 16 clear and concise requirements.
- Based on best practices and evidence of what works.
- Designed to be universal and timeless.

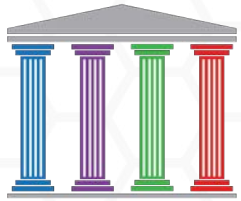
It focuses on cybersecurity programmatics: Mission Alignment, Governance, Resources, and Controls.

It is not another long list of technical requirements.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

What is a “cybersecurity program”?

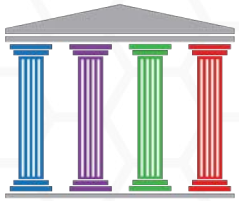
What is a cybersecurity program?



A cybersecurity program is a group of related cybersecurity-focused projects and ongoing activities managed in a coordinated way to obtain benefits not available from managing them individually. Cybersecurity programs are an organ of the larger organization, living as part of that organization through its lifecycle.

→ Adapted in part from Schwalbe, Information Technology Project Management, 9th Edition.

So, a cybersecurity program is not...

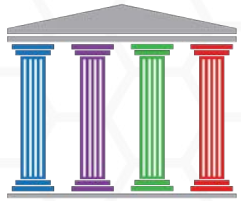


A “plan”

A “project”

A set of “controls” you are supposed to implement

Why approach cybersecurity programmatically?



Cybersecurity…

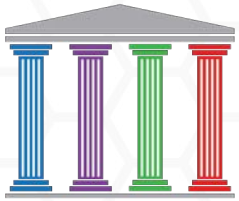
1. is dynamic, complex, and multidisciplinary.
2. takes time and resources to address competently.
3. is always relevant, regardless of where your organization is in its lifecycle.

A program supports...

1. prioritization of efforts.
2. project management; multiple projects and ongoing activities across time and space to make progress.
3. clear lines of communication, roles, responsibilities, authority, accountability.
4. resourcing.

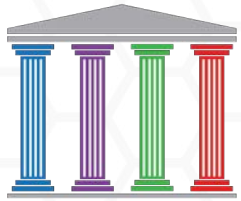
TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Enabling Cybersecurity



1. You need cybersecurity to align to the mission
2. You need people to do the cybersecurity work
3. You need money to pay for cybersecurity
4. You need leadership to set priorities and evaluate success/failure

Why Adopt?



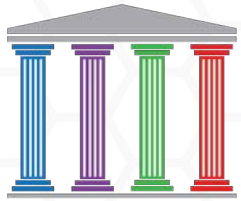
There are a lot of “frameworks” out there: why use this one?

1. It’s doable!
2. Designed to support your mission.
    a. Not checkbox compliance.
3. Built from Trusted CI’s on-the-ground experience and R&D.
    a. Addresses common barriers to effective programs.
4. Overseen by stakeholders from across the community.
5. Will enable the rest of your cybersecurity efforts.
    a. Including other frameworks + compliance.
6. Targeted at (and understandable by) organizational leadership.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Framework Adoption

Framework Cohorts



Overview:

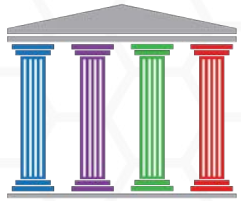
1. **Period**: 6 months
2. **Group engagement**: 4-6 organizations
3. **Goal**: Framework Adoption & Implementation

Strengths

1. Learn from/with fellow organizations
2. In-depth Trusted CI guidance
3. Lower time commitment than a full assessment

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

The Framework Cohort (cont.)



Outcomes:

1. **Framework Adoption:** Organizations will adopt the Framework.
2. **Program Evaluation**: Organizations will develop a validated self-assessment of their cybersecurity program.
3. **Strategic Plan**: Organizations will draft a Cybersecurity Program Strategic Plan that:
    i. Connects cybersecurity to the mission
    ii. Defines a cybersecurity strategy
    iii. Set out a timeline of milestones

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Participants

1. Cohort Alpha
   a. GAGE, LIGO, NOIRLab, NRAO, NSO, OOI
2. Cohort Bravo
   a. CENIC, FABRIC, NEON, SAGE
3. Cohort Charlie
   a. ARF, DSE, IceCube, GMTO, NAN, USAP
4. Cohort Delta *(current)*
   a. NCSA, PSC, SDSC, TACC, UCAR

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Resources

Framework Implementation Guide (FIG)

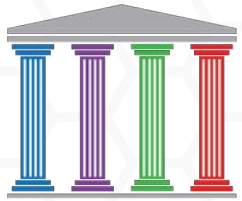
1. In-depth, audience specific guidance
2. Roadmaps, common challenges, and key resources
3. Available at: https://www.trustedci.org/framework/implementation

Updated Templates and Tools:

1. Updated Master Information Security Policy & Procedures
2. Updated Incident Response Policy
3. *New* "Cybersecurity Program Strategic Plan"
4. Available at: https://www.trustedci.org/framework/templates

Framework Highlights

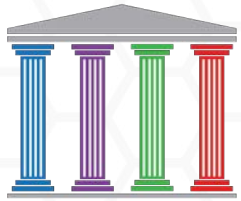
Framework Highlights: Must 5



Involve leadership in cybersecurity decision making

1. Responsibility. It is a basic principle (and often law) that these people are ultimately responsible for the organization. Some, but not all responsibility can be delegated.
2. Power. Senior leaders ultimately control the allocations of resources, budget, and personnel to support the cybersecurity program.
3. Perspective. Leaders in these roles are in the best position to adjudicate competing demands for resources across the organization, to include how much to prioritize cybersecurity.

Framework Highlights: Must 7



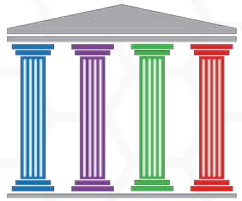
Establish a lead role with responsibility to advise and provide services to the organization on cybersecurity matters

Why is this a Must? For the same reasons you need health care providers to help you take care of your body.

1. Complexity. Cybersecurity is a complex, changing, and challenging function in any organization.
2. Impact. Cybersecurity incidents and issues can impact any part of an organization, and bring business to a halt.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Framework Highlights: Must 12

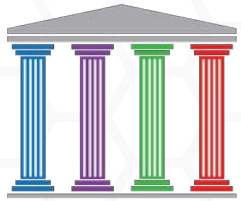


Establish and maintain a **cybersecurity budget**

Why is this a Must?

1. Informs Decision Making. Knowing how much you are spending helps evaluate the program's benefit to the mission.
2. Transparency & Rigor. Make explicit how much you are spending on cybersecurity, and have leadership approve it.
3. Organizational Commitment. A dedicated budget shows that leadership is committed to support the cybersecurity program.

Framework Highlights: Must 15



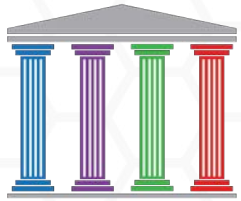
Adopt and use a **baseline control set**

You need a well-rounded diet of known-good controls.

1. Rally! Common language and structure.
2. Save resources. It relieves the resource burden of ad hoc control selection and wasted effort "reinventing the wheel."
3. Avoid gaps. A major risk of ad hoc control selection is missing important, doable controls.
4. Good baseline protection. Will address the majority of attacks.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Thank you!



Trusted CI, the NSF Cybersecurity Center of Excellence is supported by the National Science Foundation under Grant #2241313. The views expressed do not necessarily reflect the views of the National Science Foundation or any other organization.

https://trustedci.org/

info@trustedci.org
jbasney@ncsa.illinois.edu

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE