
TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE
trustedci.org

The Trusted CI Operational Technology Procurement Matrix

Developed by TCI Secure By Design Team

Speaker: Sean Peisert, Trusted CI

Nov 3, 2025, RVTEC

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

https://trustedci.org/

Trusted CI:
The NSF Cybersecurity Center of Excellence

Our mission: The mission of Trusted CI is to enable trustworthy NSF science by partnering with cyberinfrastructure (CI) operators to build and maintain effective cybersecurity programs, publishing resources that are valuable to the broader NSF community, and supporting the processes, tools, and knowledge to secure NSF research progress.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

CENTER FOR APPLIED CYBERSECURITY RESEARCH

BERKELEY LAB

PSC

ILLINOIS
NCSA | National Center for Supercomputing Applications

WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

ASU Arizona State University

SUSTAINABLE HORIZONS INSTITUTE

What are your OT procurement stories?

- Question section at the end of this webinar
- We would like to hear your own stories about security issues with OT and procurement of OT

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

What is Operational Technology (OT)?

- Connected
- Non-standard computing resources
- Part of Infrastructure
- Part of science mission
- Part of an organization's attack surface






Image credits: Sean Peisert & Mikeal Jones

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

A few historic major attacks involving OT

- Target POS breach through HVAC system (2013)
- Ukrainian Power Grid (2015)
- Colonial Pipeline attack (2021)
- Polish Train System (2023)

OT security issues

- ✗ Install & Forget
- ✗ Company is slow to update firmware
- ✗ Company out of business or one and done
- ✗ Lack of security features
- ✗ Default and hardcoded passwords
- ✗ Doesn't integrate well with existing SOC tools
- ✗ Lack of logging
- ✗ Active exploits
- ✗ Jump point to privileged network

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

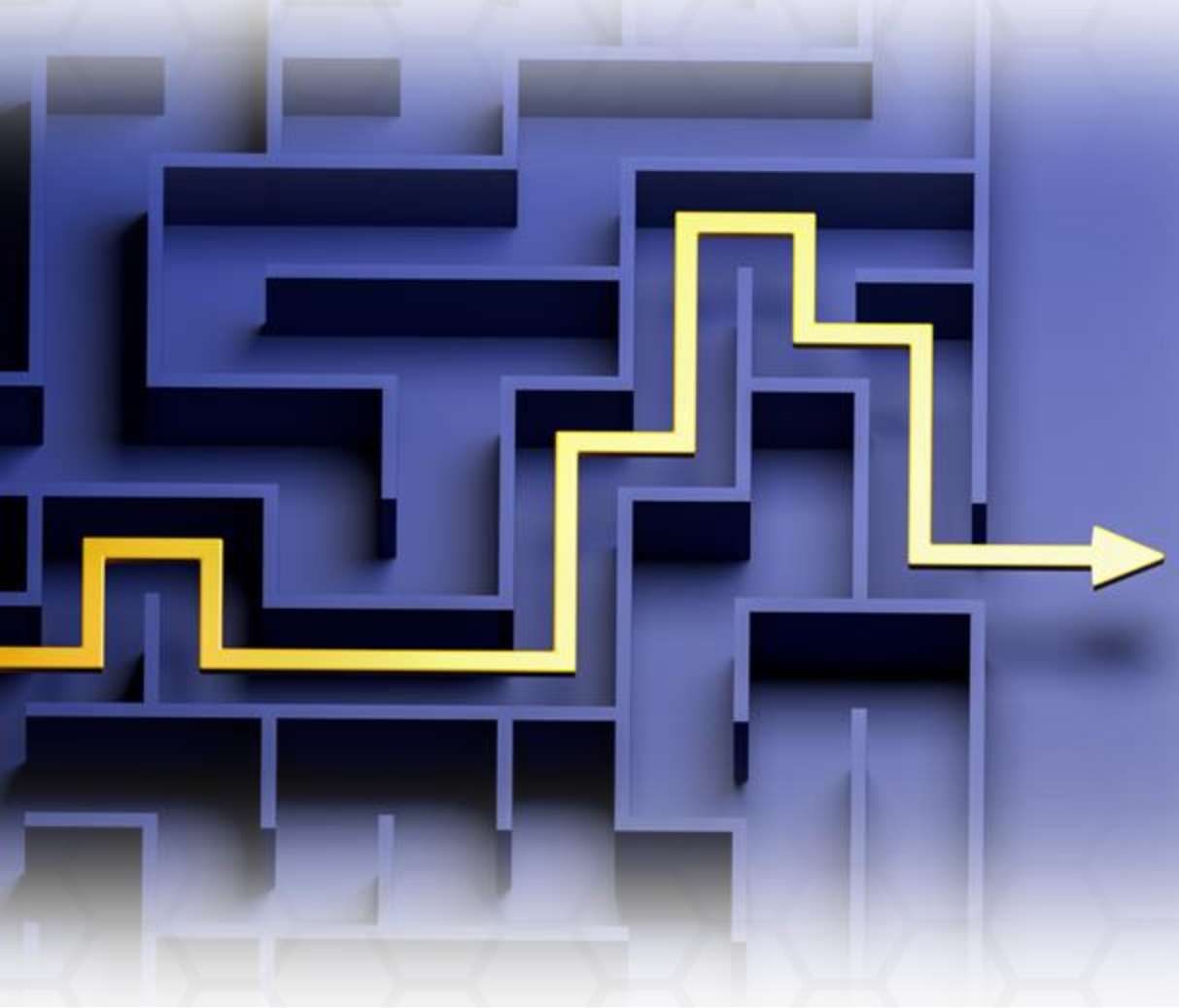
Procurement matters

- The wrong product can be hard to secure
- Lack of involvement of security staff in procurement process
- Questions aren't sent to vendor or go unanswered
- Vendor has little pressure to address issues

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Poll for the audience

- Have you run into an issue with your piece of equipment after procurement?
- Does your organization or project conduct and inventory of your operational technology assets?
- Does your IT support and cyber security program explicitly cover your OT assets or is that in a separate group?



Existing Solutions

- HECVAT & HECVAT Lite
- Ad hoc questions from each customer
- ~~[Trust the sales pitch]~~

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Why we decided to make our own

- Focus on Science needs
  - Many different sensors
  - Data integrity
  - Limited budget
  - Long procurement to production process
- No clear questionnaire tool for OT
- Need in research community for a solution
- Aligns with Trusted CI's mission

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Development process

- Brainstorming
- Gather issues
- Interviews with community
- Interview with vendor
- Review HECVAT
- Consolidate into unique questions

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Updates and what we've done since we released it.

- Revised matrix
- Created use guide
- Promoted and tracked use
- Panel discussions
- Future changes

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

The questionnaire matrix

	ID #	Control	CIS Safeguards Reference	Implementation Group	Requirement	Vendor Question:	Tips & Examples	MITRE ATT&CK [referer	Impacted MITRE ATT&CK Techniques (See CIS Community Defense Model v2.0 for additional information)
2	001	Inventory	1.1	1	Have an inventory that details network and computer hardware.	Does the product include a hardware manifest which details all computer and network hardware included?	An inventory should include physical computing assets which are components of the delivered system such as network switches, computers, or firewalls.	DS0039 [1] T0838 [2] T0836 [3] T0843 [4] T0848 [5]	Modify Alarm Settings, Modify Parameter, Program Download, Rogue Master
3	002	Inventory	2.1	1	Provide a software bill of materials (SBOM) for the product.	Provide a software bill of materials (SBOM) for the product.	Ensure that no unauthorized software is used/enabled. Specifically identify and document software which accepts network connections.	M0817 [18 DS0039 [9] T0862 [10]	I/O Image, Manipulate I/O Image, Modify Controller Tasking, Modify Program, Supply Chain Compromise
4	003	Inventory	2.2	1	Security vulnerabilities in vendor provided software must be patched.	Will the product receive software security patches throughout the product's intended lifecycle?	Describe the expected patching cycle for security vulnerabilities discovered in the product, the recommended patching timetable, and the patching method used.	M1051 [14]	Abuse Elevation Control Mechanism, Malicious Browser Extensions, Bypass User Account Control, TCC Manipulation, Brute Force: Password Guessing, Credentials from Password Stores, Password Managers, Data from Configuration Repository, Drive-by-Compromise, Event Triggered
5	004	Inventory	2.2	1	Software must run on supported versions of operating systems throughout the intended product lifecycle.	Will software components of the product be supported on operating systems supported by the operating system vendor throughout the product's intended lifecycle?	Do not use end-of-life operating systems such as Windows XP, Server 2003 or Vista. They no longer receive security patches and are vulnerable to compromise.	M0928 [16] M0954 [17]	Autorun Image, Replication Through Removable Media
6	005	Data Protection	3.3	1	The product must provide a mechanism to prevent unauthorized access to data.	Can access to data be restricted to prevent unauthorized access?	File system permissions are a simple and widely supported mechanism for accomplishing this.	M0801 [18] M0927 [19] M0922 [20]	Activate Firmware Update Mode, Change Operating Mode, Default Credentials, Detect Operating Mode, Device Restart/Shutdown, Execution through API, Hardcoded Credentials,
7	006	Secure Configuration	4.6	1	Remote maintenance must use secure communication channels.	Are all communications methods used for remote maintenance using encryption?	Use secure communications methods such as SSH or HTTPS for remote maintenance activities.	T0822 [22]	External Remote Services
					It must be possible to either change credentials of or disable	Can default accounts be disabled or their credentials changed, including encryption keys?	For operating system accounts such as Windows accounts, the	T1078.001 [24]	Account Manipulation, Create Account, OS Credential Dumping, Remote

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

https://www.trustedci.org/secure-by-design

Matrix: https://zenodo.org/records/13830599

Matrix guide: https://zenodo.org/records/13743314

The questionnaire matrix (Part 2)

	A	B	C	D	E	F	G	H	I
1	ID #	Control	CIS Safeguards Reference	Implementation Group	Requirement	Vendor Question:	Tips & Examples	MITRE ATT&CK [refere	Impacted MITRE ATT&CK Techniques (See CIS Community Defense Model v2.0 for additional information)
8	007	Secure Configuration	4.7	1	It must be possible to either change credentials of or disable any default accounts.	Can default accounts be disabled or their credentials changed, including encryption keys?	For operating system accounts such as Windows accounts, the built-in password change mechanisms are sufficient to qualify. Other accounts such as web application accounts should also be possible to change.	T1078.001 [24]	Account Manipulation, Create Accoun OS Credential Dumping, Remote Desktop Protocol, Domain Accounts, Command and Scripting Interpreter, Brute Force, Valid Accounts, Window Service, Default Accounts,
9	008	Secure Configuration	4.8	2	It must be possible to disable services or functionality which is not necessary for the proper functionality of the product in its installed application.	Can unused functionality be disabled such that it is unavailable?	This can be achieved by a variety of means, including disabling services, uninstalling software, disabling software which listens on network ports, or explicitly blocking port numbers using host firewall rules.	T1210 [26]	Exploitation of Remote Services
10	009	Account Management	5.2	1	Accounts must use unique credentials or it must be possible to configure them to use unique	Can all accounts be configured to use different credentials?	Use unique passphrases or keys for each account.	T1110.004 [29]	Credential Dumping, Valid Accounts, Domain Accounts, Brute Force
11	010	Account Management	5.3	1	Disable unused accounts	Can accounts be disabled, including unused default accounts?	This should apply to operating system accounts as well as other accounts on the system. Built-in mechanisms for disabling Windows or Linux accounts can be used to meet this requirement.	M0936 [31]	Account Manipulation, Create Accoun OS Credential Dumping, Remote Desktop Protocol, Domain Accounts, Command and Scripting Interpreter, Brute Force, Valid Accounts, Window Service
12	011	Account management	5.4	1	Users of the system must use accounts with limited privileges when logging in.	Can user accounts have their privileges restricted?	"Administrator" or "root" accounts should not be used as day-to-day user accounts on computer systems. Windows and Linux systems provide the ability to operate with reduced privileges via UAC and sudo mechanisms respectively.	M0926 [32]	Account Manipulation, Create Accoun OS Credential Dumping, Domain Accounts, Command and Scripting Interpreter, Valid Accounts, Windows Service
					Remote network access requires multifactor authentication.	Does the product support multifactor authentication for remote access?	Institutional policy and procedures may define specific allowed or required multifactor	T1110 [34] M1032 [35]	Account Manipulation, Create Accoun Remote Desktop Protocol, Domain Accounts, Brute Force

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

https://www.trustedci.org/secure-by-design

Matrix: https://zenodo.org/records/13830599

Matrix guide: https://zenodo.org/records/13743314

The questionnaire matrix (Part 3)

	ID #	Control	CIS Safeguards Reference	Implementation Group	Requirement	Vendor Question:	Tips & Examples	MITRE ATT&CK [refere	Impacted MITRE ATT&CK Techniques (See CIS Community Defense Model v2.0 for additional information)
17	016	Audit log management	8.2	1	The product must produce logs which provide necessary information for event analysis and incident investigations. At minimum, these must include system logins and usage of elevated privileges.	Does the product keep a record of important events, particularly login activity and usage of elevated privileges?	Minimally, events indicating successful/failed authentication attempts and usage of elevated privileges must be collected. It may also be important to collect additional items such as DNS lookups, command line execution logs, URL request logs, encryption certificate details, or API request details.	T1027.005 [44] T1562.002 [45] T1562.003 [46] T1654 [47]	Indicator Removal on Host, Disable Windows Event Logging, Impair Command History Logging, Log Enumeration
18	017	Audit log management	8.9	2	Logs from the system must be able to be forwarded to a central logging system.	Does the product store logs in a way that allows them to be forwarded to log aggregation systems?	Sending logs and alerts to a central repository enables faster detection of issues and ensures records are available after an incident has occurred.	T1027.005 [49] T1562.002 [50] T1562.003 [51] T1654 [52]	Indicator Removal on Host, Disable Windows Event Logging, Impair Command History Logging, Log Enumeration
19	018	Malware defenses	10.1	1	Deploy anti-malware software and enable it.	Does the product allow for the installation of anti-malware software on common operating systems which are network connected?	Built-in offerings such as Windows Defender qualify for this requirement.	T1543 [54] T1059 [55] T1027 [56] T1014 [57]	Create or Modify System Process, Command and Scripting Interpreter, Obfuscated Files or Information, Rootkit
20	019	Malware defenses	10.2	1	Configure automatic updates for anti-malware software	Can malware definitions be updated automatically where applicable?	As malware techniques change over time, anti-malware defenses must change as well. Definition updates must be enabled in order for the	TA0003 [59] T1098 [60] T1059 [61] T1027 [62]	Account Manipulation, Command and Scripting Interpreter, Obfuscated File or Information
21	020	Malware defenses	10.3	1	Disable autorun and autoplay for removeable media	Do any computer systems which are components of the product have autorun or autoplay enabled for removeable media?	There are multiple "autorun" and "autoplay" mechanisms in modern operating systems that are important to take account of. For example, Microsoft sysinternals includes the "autoruns" utility, which is a useful way to check these on Windows systems: Link [20]	T1119 [63] T1092 [64]	Automated Collection, Communicatio Through Removable Media
					There must be a mechanism available to automatically back up	Are there backup mechanisms in place which can be used to automatically back up and restore data	Software configuration files are a common example of data	TA0010 [66]	Exfiltration

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

https://www.trustedci.org/secure-by-design

Matrix: https://zenodo.org/records/13830599

Matrix guide: https://zenodo.org/records/13743314

The questionnaire matrix (Part 4)

ID #	Control	CIS Safeguards Reference	Implementation Group	Requirement	Vendor Question:	Tips & Examples	MITRE ATT&CK [referer	Impacted MITRE ATT&CK Techniques (See CIS Community Defense Model v2.0 for additional information)
019	Malware defenses	10.2	1	Configure automatic updates for anti-malware software	Can malware definitions be updated automatically where applicable?	As malware techniques change over time, anti-malware defenses must change as well. Definition updates must be enabled in order for the	TA0003 [59] T1098 [60] T1059 [61] T1027 [62]	Account Manipulation, Command and Scripting Interpreter, Obfuscated Files or Information
020	Malware defenses	10.3	1	Disable autorun and autoplay for removeable media	Do any computer systems which are components of the product have autorun or autoplay enabled for removeable media?	There are multiple "autorun" and "autoplay" mechanisms in modern operating systems that are important to take account of. For example, Microsoft sysinternals includes the "autoruns" utility, which is a useful way to check these on Windows systems: Link [20]	T1119 [63] T1092 [64]	Automated Collection, Communication Through Removable Media
021	Data Recovery	11.2	1	There must be a mechanism available to automatically back up and restore data necessary for the product to function. This restoration mechanism should be available to the responsible staff without third-party intervention under degraded operating conditions.	Are there backup mechanisms in place which can be used to automatically back up and restore data necessary for the product to function? Can this mechanism be used to restore functionality by authorized staff without outside intervention?	Software configuration files are a common example of data necessary for products to function. Standard backup and recovery mechanisms such as Windows backup or rsync can often be configured to suffice for this requirement.	TA0010 [66]	Exfiltration
022	Network Infrastructure Management	12.1	1	Network devices which are includec as components of the product should be capable of being patchec	Do all network devices included with the product provide a mechanism of patching security vulnerabilities?	i.e., vpn, router and/or switch firmware	TA0004 [69] T1190 [70] T1133 [71]	Privilege Escalation, Initial Access, Persistence
023	Network Infrastructure Management	12.4	2	Provide a network diagram describing the system components and their interaction mechanisms.	Does the product documentation include a network diagram describing key networked components and their interactions?	Documentation is important to ensuring all aspects of the network are properly configured. This documentation would prove invaluable when upgrading/repalcing components.	T5190 [73] T1595 [74]	Active Scanning, Network Trust Dependencies
	Version: 2024-09-							

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

https://www.trustedci.org/secure-by-design

Matrix: https://zenodo.org/records/13830599

Matrix guide: https://zenodo.org/records/13743314

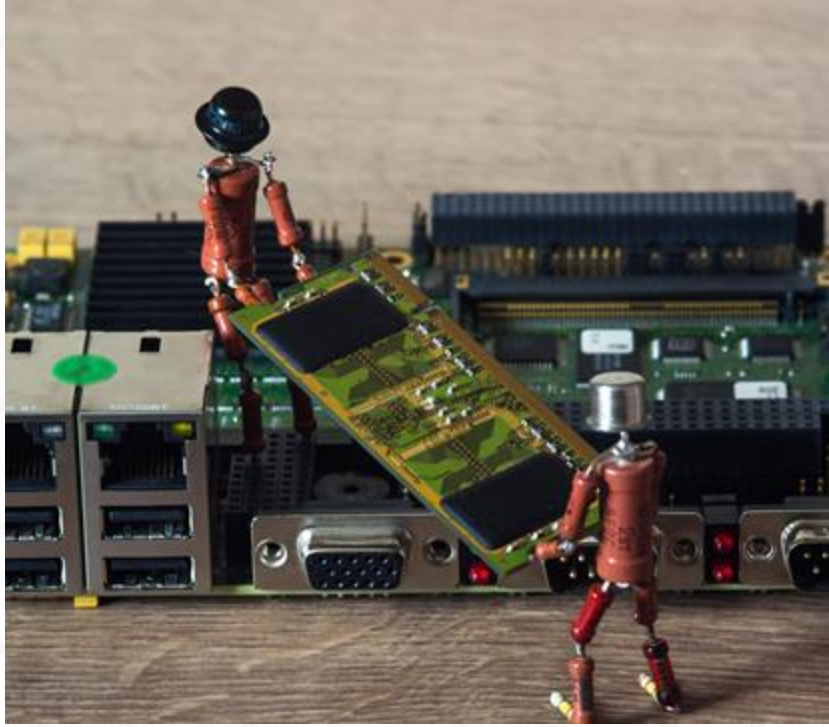
Sample question:

#5

- Related CIS control: 3.3
- Requirement: The product must provide a mechanism to prevent unauthorized access to data.
- Question: Can access to data be restricted to prevent unauthorized access?
- Example answers:
  - Yes, the control interface requires a numeric pin to be entered to access data

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Sample question:



#22

- Related CIS control: 12.1
- Requirement: Network devices which are included as components of the product should be capable of being patched to fix security vulnerabilities.
- Question: Do all network devices included with the product provide a mechanism of patching security vulnerabilities?
- Example answers:
  - Yes, there is a web interface where you can upload new firmware, which is available from updates.companyname.com
  - Yes, you will need to subscribe to a support plan for access to updates
  - No, we fired our programming staff after making the product

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Using the Matrix

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

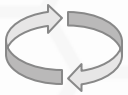
How to use the questionnaire matrix: Summary of Major steps

1.

Prepare
customizations as a team

2.

Distribute
to vendors



2.1

Conduct Q&A
with vendors & team members iteratively

3.

Team review
of vendor responses, requests clarification as needed

4.

Final review
and comparison involving Risk Officer to select vendor(s)

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Step 1: Prepare as a team

Who to involve

- Facility leadership
- IT & OT technical staff
- Project management staff
- Procurement staff

Team should identify who will be responsible for addressing particular types of vendor questions.

Examples include technical staff such as cybersecurity plus the appointed Risk Officer.

What to do

1. Review the Matrix questions
2. Identify which are relevant
   a. Not everything is applicable
   b. Some things may require more detail
   c. Certain certifications (e.g., ISO) may or may not be important
3. Customize Matrix for current procurement

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Step 2: Distribute to vendors

Procurement lead distributes customized Matrix to vendors

Set expectations for Q&A between vendor and team

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Step 2.1: Vendor Q&A

- Procurement team carefully evaluates vendors' responses
- Determine if responses are acceptable based on your cybersecurity program
  - don't hesitate to reach out for support, e.g., Trusted CI, if a vendor response appears obfuscated or confusing
- Draft clarifications or additional questions and re-submit to vendor(s)
  - consider this a form of negotiation
- Record/document all the team's decisions/progress

Step 3: Team reviews responses

- Review responses for conflicting or unclear information
  - Develop clarifying questions to send back to vendor
- For "no"s, determine if a mitigating control can be used
- Compare the risk of product based on “no”s along with their mitigating controls, to alternative products if available
- Find a balance between accepted risk and mitigated risk suitable for completing the mission
- Keep in mind that science is the mission

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Step 4: Final review

- Seek Additional Details and Clarification As Necessary
- Discuss Internally and Perform Risk Assessment
- Develop Plan to Implement Mitigating or Compensating Controls
- Plan for Obsolescence
- Procure?
- Develop Asset/Integration Management Plan

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Resources

The Matrix: https://trustedci.org/ot-matrix

Google Sheets Version: https://trustedci.org/ot-matrix-sheet

The Guide to the Matrix: zenodo.13743313

The Matrix One-Pager: OT-Matrix-One-Pager.pdf

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Questions

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE