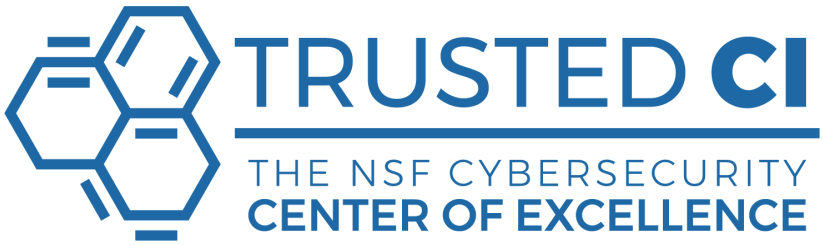


Guide to Using the Trusted CI OT Procurement Matrix

NSF Grant OAC-2241313

September 23, 2024

For Public Distribution

Andrew Adams,[1] Dan Arnold,[4] Jeannette Dopheide,[3] Shane Filus,[1] Mikeal Jones,[2] Mark Krenz,[2] Drew Paine,[4] Sean Peisert,[4] Michael M. Simpson,[2] and John Zage[2]

1 Carnegie Mellon University/Pittsburgh Supercomputing Center (PSC)

2 Indiana University/Center for Applied Cybersecurity Research (CACR)/OmniSOC

3 University of Illinois/National Center for Supercomputing Applications (NCSA)

4 Lawrence Berkeley National Laboratory

About Trusted CI

Trusted CI is funded by NSF's Office of Advanced Cyberinfrastructure as the NSF Cybersecurity Center of Excellence (CCoE). In this role, it provides 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 an effective cybersecurity program. Trusted CI achieves this mission through a combination of one-on-one engagements with NSF projects, training and best practices disseminated to the community through webinars, a Fellows program, and the annual, community-building NSF Cybersecurity Summit for Major Facilities (MF) and Cyberinfrastructure.

For information about Trusted CI, please visit the project website: https://trustedci.org

To reference the Trusted CI project, please reference the following paper:

> Andrew Adams, Kay Avila, Jim Basney, Dana Brunson, Robert Cowles, Jeannette Dopheide, Terry Fleury, Elisa Heymann, Florence Hudson, Craig Jackson, Ryan Kiser, Mark Krenz, Jim Marsteller, Barton P. Miller, Sean Piesert, Scott Russell, Susan Sons, Von Welch and John Zage. Trusted CI Experiences in Cybersecurity and Service to Open Science. PEARC'19: Practice and Experience in Advanced Research Computing, 2019. https://doi.org/10.1145/3332186.3340601

About This Report

This document is the product of Trusted CI, The NSF Cybersecurity Center of Excellence, and was supported by the NSF under award number 2241313.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Please cite this report as:

> Guide to Using the Trusted CI Operational Technology Procurement Vendor Matrix. September 2024. https://doi.org/10.5281/zenodo.13743314

For updates to this report and other reports from Trusted CI, please visit https://trustedci.org/reports/

Table of Contents

1 About the Matrix

In 2023, Trusted CI initiated an effort to help address the unique cybersecurity challenges that exist when a NSF research project has a strong reliance on operational technology (OT). After investigating multiple NSF Major Facilities (MFs), the study team stumbled upon a reoccurring issue: an inability of the procurement process to ensure that the necessary cybersecurity controls were included in purchased OT. Looking into this issue further, several of the individuals involved in procurement at the MFs alluded to desiring some level of guidance in knowing what cybersecurity controls are essential, and thus, what questions to ask of vendors during the procurement process. It also became clear in these conversations that not only did those individuals involved in procurement want to know which cybersecurity controls were necessary, but also *why* they were important, the latter, in order to justify their demands with the vendors. Hence, the production of the Trusted CI OT Procurement Matrix[1]; a list of essential controls for OT connected to research cyberinfrastructure, each associated with what to ask of a vendor to ensure the control is satisfied, but also why this control is essential.

1.1 Accessing the Matrix

The Trusted CI OT Procurement Matrix is a spreadsheet that can be downloaded and customized at the URL linked below:

https://zenodo.org/doi/10.5281/zenodo.10257812

2 Overview and Goals

The OT Procurement Vendor Matrix, henceforth referred to as the "Procurement Matrix," is a list of important security concepts and controls. Each of the concepts and controls has associated fields to explain both its importance and definition and suggestions on how to ask a vendor about how each is implemented or fulfilled in a device or system being procured. We will define each of these fields later. Although the Procurement Matrix refers to and was influenced by the Center for Internet Security's (CIS) guidance documents, including the CIS Controls v8[2], the security concepts and controls listed could be mapped to specific items in the guidance from many of the major organizations in the field, including NIST, ISO[3], and ISA[4] publications. By focusing at a more conceptual level, the Procurement Matrix is a tool to help inform and build other documents used to interact with vendors when procuring devices or systems for the operation of a research facility. Examples of the documents that could be

[1] https://zenodo.org/doi/10.5281/zenodo.10257812
[2] https://www.cisecurity.org/controls/v8
[3] https://www.iso.org/standard/iso-iec-27000-family
[4] https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

assisted by use of the Procurement Matrix are Request for Proposals (RFP)/Request for Quotes (RFQ), questionnaires for vendors to answer as a follow up to submitted RFP/RFQ responses, and agendas for meetings with vendors for focusing on security.

This makes the Procurement Matrix different from full questionaire-like tools, such as EDUCAUSE's HECVAT[5], in that the Procurement Matrix allows for the creation of other documents to initiate or further discussion on security concepts and controls with multiple people at several phases of procurement, implementation, and integration. The Procurement Matrix could be used to create a vendor/device- and facility-specific questionnaire like the HECVAT (see comparison table in section 2.1), but more focused on specific vendors, device types, and your facility.

The Procurement Matrix fields include: ID #, Control, CIS Safeguards Reference, Implementation Group, Requirement, Vendor Question, Tips & Examples, Threat Actor Examples, and three Reference Links. <insert bulleted dictionary of fields, with additional explanation>

2.1 Distinctions from HECVAT

The following table shows some of the similarities and differences between the Procurement Matrix and the HECVAT Full and HECVAT Lite.

	Trusted CI OT Procurement Matrix	**HECVAT Full 3.05**	**HECVAT Lite 3.05**
Target audience	Operational Tech Vendors	Cloud service vendor	Cloud service vendor
Main beneficiary	Research Facilities	Institutions of Higher Education	Institutions of Higher Education
Format	Spreadsheet	Spreadsheet	Spreadsheet
Primary Asset Focus	Operational Technology	Cloud Applications / Services	Cloud Applications / Services
Number of questions for vendors	23	238	78
Usage	Customer chooses appropriate questions to pose to vendor	Vendor completes HECVAT	Vendor completes HECVAT
Goals	Inform the customer	Inform Higher Ed about	Similar to HECVAT full, but

[5] https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit

	about potential security risks, security integration issues, and security features or shortcomings of a product; To increase the likelihood that important cybersecurity issues are brought up during procurement; Bring consistency to questions posed to vendors.	provider practices to help prevent data breaches; Make it easier for vendors by unifying answers in a consistent way, from which all institutions can learn about vendor practices.	with reduced depth of questions in certain areas. Not as focused on critical data.
Compliance standards referenced in questions	CIS Controls	PCI DSS; HIPAA; ISO 27001; NIST Cybersecurity Framework; CIS Critical Security Controls	PCI DSS; HIPAA; ISO 27001; NIST Cybersecurity Framework; CIS Critical Security Controls
Focuses on cyber risks to physical assets	Yes	No	No
Provides threat actor examples per question	Yes	No	No
Provides mitigation tips per question	Yes	No	No

3 Who Should Use the Procurement Matrix

The Procurement Matrix is intended for those involved in all stages of the procurement process. This includes those who request, review, purchase, install, maintain, and secure OT assets. An example scenario might involve an electric crane intended for a maritime research vessel. Ship operations staff may request the purchase of the crane and consult the Procurement Matrix to determine features that they should look for in product literature or when talking to product sales. Project leadership, who accepts the cybersecurity risk for the organization, can consult the Procurement Matrix to know what potential risks may be present when purchasing operational technology and assign staff to investigate further. The purchasing department can talk with the crane vendor's sales department in coordination with cybersecurity staff for the project, so project leadership can be sure that cybersecurity questions are properly addressed by the vendor prior to purchase. The cybersecurity staff can use the Procurement Matrix to determine some of the common risks they should consider with the asset and if needed, protect the asset with compensating controls.

4 How to Use the Procurement Matrix

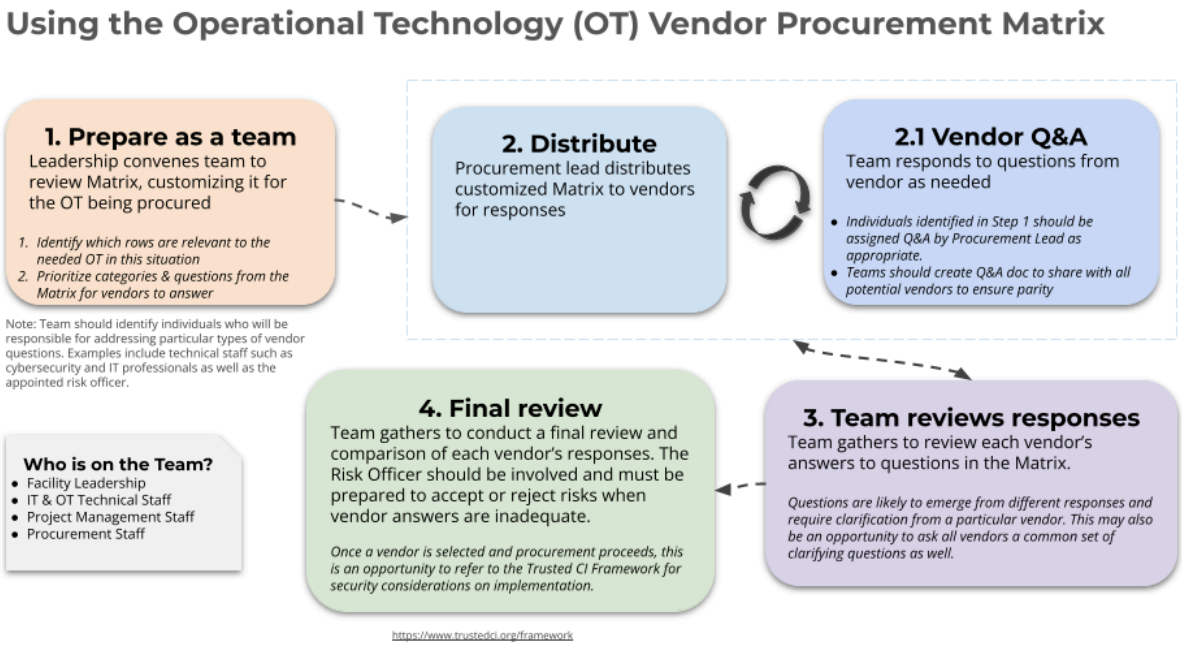
We encourage users to do some preparation work prior to sending the questionnaire to vendors, including reviewing the questions and related controls in the questionnaire, determining which rows apply to the technology to be procured, and considering the priority of each row. Upon sending the questionnaire to a vendor, our experience suggests expecting extended wait times for completion, even up to a month. While waiting for the completion of the questionnaire, it can be helpful to identify personnel who will review vendor responses. Useful reviewers typically include technical staff such as cybersecurity and IT professionals, and the appointed risk officer, who must be able to accept risk or make decisions to mitigate the risk choosing the vendor should the vendor's answers not all be satisfactory.

4.1 Step-by-Step

Stages:

1. Preparation
    a. Review as a team, identify any potential adaptations to Procurement Matrix questions before sharing with vendors
    b. Technical Requirements, including integration w/other components
    c. End-user needs
    d. Costs
2. Distribution of questionnaire
    a. Set expectation of Q&A between vendor and team
    b. Select personnel to prepare to review vendor responses
3. Team review of vendor responses
    a. Decision-making
    b. Circulation of additional questions to vendors for clarification
4. Comparison of vendor responses
    a. Determine which vendor to proceed with through procurement process

4.2 Visual Walkthrough



5 Example Use Case – SasqWATCH

SasqWATCH, a fictitious science project dedicated to discovering proof of the existence of the Sasquatch and other cryptids, requires advanced electronic equipment to enhance their field research capabilities. Among the crucial tools needed is a remote-controlled drone equipped with high-resolution cameras and thermal imaging technology, facilitating aerial reconnaissance of remote and rugged terrain. Recognizing the importance of cybersecurity in safeguarding sensitive data and ensuring the reliability of operations, SasqWATCH initiates a rigorous vendor selection process. To evaluate the security posture of potential vendors, SasqWATCH uses the Trusted CI OT Procurement Vendor Procurement Matrix to formulate questions outlining necessary cybersecurity controls and their significance. When the first vendor candidly admits their lack of security awareness and suggests consulting a more security-minded vendor, SasqWATCH takes heed. In contrast, the third vendor, dubbed *GuardianTech*, demonstrates proactive engagement by meticulously reviewing the questionnaire, updating their security documentation accordingly, and providing detailed responses addressing each inquiry. Impressed by GuardianTech's commitment to security and responsiveness, SasqWATCH confidently selects them as their vendor of choice, ensuring the acquisition of equipment not

only advances their Sasquatch research but also fortifies their cybersecurity defenses against potential threats.

6 Additional Resources

6.1 HECVAT

HECVAT

https://www.ren-isac.net/public-resources/hecvat.html

Higher Education Community Vendor Assessment Toolkit | EDUCAUSE Library

The Higher Education Community Vendor Assessment Toolkit (HECVAT) is a vendor risk management framework questionnaire tailored to higher education environments. The vendor questionnaire can help institutions make informed decisions related to cyber risk and impact to their organization. HECVAT was developed by collaboration between the Higher Education Information Security Council (HEISC), REN-ISAC and Internet2.

6.2 CIS Controls

CIS Controls

https://www.cisecurity.org/controls

CIS Controls, constructed by the Center for Internet Security, provides a prioritized set of defensive actions aimed to protect organizations from the most common attacks. Controls are made up of smaller actions called “Safeguards.” CIS created “Implementation groups (IG)” to help organizations prioritize safeguards.

7 How to Submit Feedback About the Procurement Matrix

Our goal is to share the Procurement Matrix and continue to develop its utility after receiving feedback from the Trusted CI community. To contact us, email info@trustedci.org.

8 Acknowledgements

This document represents the work of many people, including critical feedback from maritime OT practitioners (Scripps Institution of Oceanography's CCRV[6] and Oregon State University's RCRV[7] and OOI[8]). We are grateful for their contributions to this effort.

[6] UC San Diego Receives $35 Million in State Funding for New California Coastal Research Vessel
[7] https://ceoas.oregonstate.edu/regional-class-research-vessel-rcrv
[8] https://oceanobservatories.org/