PROTECT OUR POWER

**Best Practices in Cybersecurity for Utilities:**
Criteria Discussion

https://protectourpower.org/best-practices/pop-bp-criteria-discussion.pdf

## Introduction:

This paper is an attempt to capture information related to Criteria in the Protect Our Power Project called "Best Practices in Cybersecurity for Utilities" – BP Project. Criteria make up the columns in a Vendor Comparison Matrix. Criteria are the body of individual criterion that a Utility would look to for making buying decisions.

The BP Project has the following guiding Mission:

1. Help the Utilities move faster to deploy best practices in cybersecurity.
2. Help the Utilities move in the direction of best practices.

Criteria contribute to this Mission directly. By initially answering (via unbiased scoring by Universities) buying-questions (criteria), a Utility is able to move quicker to select a small number of Vendors for consideration. The fact that each criterion will have a utility-controlled weighting helps to ensure both specific utility appropriateness and movement towards best practices (the better vendors for a specific utility).

## Advisory Board[1] – Criteria:

ProtectOurPower.org has an Advisory Board that meets monthly (via conference call) to discuss the all-important Criteria related to the comparison of Vendors. While the Advisory Board existed before 2020, it was not activated until early 2020.

A separate document describing the Advisory Board for Criteria is available. There is also a page on the Protect Our Power website for the Criteria Advisory Board.

[1] Industry members interested in participating in the Project Advisory Board can contact Erick Ford (eford@protectourpower.org)

## Criteria – Two Buckets:

Two main categories of Criteria exist – those that are standard and generally apply to all Topic areas[2], and those that are Topic specific. Criteria establish the columns in the Comparison Matrix and are an input the selected Educational Institution selected to develop Work Products[3] for a Topic. We are using the terms: Common Criteria and Topic-Specific Criteria to represent these two buckets of Criteria

## Criteria Types – Two Buckets:

In addition to thinking about Criteria as Common and Topic-Specific – the Project recognizes that some criteria will be binary and some more amenable to scoring (by the University).

***Binary Criteria*** are buying considerations that are best addressed with a "Yes" or "No". For example – "Do you have a reference customer that is an electric utility?" or "Do you have a supply chain document you will share with utilities that addresses your supply chain security?"

***Scoring Criteria*** are buying considerations that can be addressed via a score to provide the utility with a sense of capability withing specific criterion for each Vendor in the Vendor Comparison Matrix.

Therefore, Criteria can be thought of fitting into one of the following four quadrants:

| | |
|---|---|
| **Common Criteria / Binary Criteria** | **Common Criteria / Scoring Criteria** |
| **Topic-Specific Criteria / Binary Criteria** | **Topic-Specific Criteria / Scoring Criteria** |

## Supporting Documents:

Common Criteria Workbook – provides information related to specific Common Criteria - https://protectourpower.org/best-practices/pop-bp-criteria-common.xlsm

[2] The Topics are defined in the Taxonomy as well as the Vendors under each Topic.

[3] See ***Educational Institutions – Work Product Requirements*** - https://protectourpower.org/best-practices/pop-bp-ei-work-products.pdf

## University Implications:

Protect Our Power relies on Educational Institutions to be unbiased evaluators of Vendors using Criteria (things of decision-making interest to the Utilities). The Educational Institutions are final arbiters of which Criteria to use and how to evaluate (score or reach a binary decision) each criterion within that set.

## Common Criteria:

A separate Excel Workbook is being maintained to include information related to suggested Common Criteria. Educational Institutions should lean in the direction of using virtually all of these Criteria in order to maintain some consistency (important to the Utilities) across Topics.

## Topic-Specific Criteria:

A separate Excel Workbook is being maintained to include information related to suggested Common Criteria. Educational Institutions should lean in the direction of using virtually all of these Criteria in order to maintain some consistency (important to the Utilities) across Topics.

## Criteria References:


1. ***2019 CWE Top 25 Most Dangerous Software Errors*** - https://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html - a criterion is having each Vendor certify (indicate by email) that their software does not include any of the errors mentioned.
2. ***Best Practices in Vendor Selection and Management*** - https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-SCRM-Vendor-Selection-and-Management.pdf
3. ***Comparison of Antivirus Software*** - https://en.wikipedia.org/wiki/Comparison_of_antivirus_software - example of a matrix with defined criteria
4. ***Comparison of Dragos community tools*** - https://dragos.com/community-tools
5. ***Cyber Resilience Review (CRR): Question Set with Guidance*** – 2016-02-01 - https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-question-set-and-guidance.pdf

6. ***FireCompass Third Party Risk Management Checklists and Frameworks from the Web*** - https://www.firecompass.com/blog/free-third-party-risk-management-checklists-and-frameworks
7. ***MAP01 -*** Indegy PDF showing the proper mapping of their product - https/EnergyCollection.us/Companies/Indegy/Adhering-NIST-Framework.pdf
8. ***Top 10 Questions in Vendor Cybersecurity Questionnaires*** - https://www.venminder.com/blog/top-10-questions-vendor-cybersecurity-questionnaires

**Next Steps:**

Anyone interested in discussing or contributing to the Criteria discussion should contact Erick Ford (eford@protectourpower.org). Contributions, criticisms, and other comments are welcome.

**Contact**
**Erick Ford | Project Manager**
eford@protectourpower.org