## DWF CNA Planning Discussion Points

We believe the proposal regarding DWF accurately captures the pilot plan discussed in our last Editorial Board meeting. We would like to clarify that we consider this to be a pilot of DWF as a CNA, rather than an integration of DWF and CVE as stated in the language of the proposal. Our reason for making this clarification is that we believe the DWF CNA pilot may lay the foundation for other use-case specific or domain-specific organizations to join as CNAs in the future, and thus expand the reach and impact of the CVE program. Below we outline several talking points that we would like to work through with the Editorial Board. In general, these talking points seek to clarify the boundaries of the pilot, the level of integration with the existing CVE program, and the criteria by which we are evaluating the DWF CNA Pilot.

1. What criteria would the EB like to evaluate the pilot against? (e.g., counting, duplicates.)
    - Why this matters: Without any objective criteria for evaluation, it will be difficult to understand whether or not we are successful. Identified criteria will help us determine if we are meeting the needs of all CVE uses cases. Also, some of the criteria may require creating additional capabilities as part of the pilot, e.g. a feedback form.

2. How does the pilot compare to the current CVE processes?
    - Why this matters: A complete understanding of the differences in processes up front is essential to ensure that we understand the downstream effects as well as the modifications that would be required to merge the data into the production stream.

3. How do we measure the success of the DWF pilot with regard to the ID-only and existing use cases?
    - Why this matters: Without any specifics for how to measure success or failure of the pilot program, it will be difficult to make progress. Also, we must consider all the use cases to prevent negatively affecting any of them in the process of improving service to one. Finally, by identifying what the Editorial Board and the CVE team expect to get from the pilot, the DWF team will know what is expected of them.

4. What are the boundaries and areas of responsibility for what DWF will cover and what the CVE team should cover? For example, should DWF handle Linux distributions and their packages? If so, which distributions? Default packages, or all? What happens when DWF accidentally assigns a CVE for an issue in the CVE Team scope, and vice versa?
    - Why this matters: Open source software is a very large category that could overlap with many existing CNAs' responsibilities. Clear boundaries matter as they avoid duplicate efforts on the part of DWF and the CVE Team, as well as avoid duplicate CVE assignments when a requester sends a request to both at the same time. Who should handle such a request? According to what guidance and rules? Another reason to worry about boundaries, at least initially, is that CVEs assigned by DWF will

look and possibly be handled differently from CVE Team-assigned CVEs. Also, clear boundaries will allow for operational efficiencies, giving CVE and DWF staff clear instructions as to where to redirect requests that are sent to the inappropriate entity. Even with clear boundaries, violations will occur. By defining a resolution process now, we will avoid problems down the road and increase the likelihood of success for the pilot.

5. How should the DWF data be handled? Should these new CVEs be made available through GitHub? Should the CVEs be separated from one another? (e.g., separate feeds.)
    - Why this matters: As with any experiment, we need to understand what the controls are as well as the variables being introduced. The way the CVE Team handles the DWF assigned CVEs will have a significant impact on the results of the pilot. If the CVE Team merges the DWF CVEs into the CVE download, many more people will become aware of the assignments but it will also make rolling back the CVEs more difficult if the pilot fails. If we add these new CVEs and they are different in some ways (e.g., no description), this may cause problems with the current downstream users. NVD has already pointed out that they will need to do a lot more work in order to add CPE, CVSS, CWE information. We need to understand how the pilot affects the operational environments of our stakeholders/consumers, as well as their stakeholders and consumers.

6. What is the expectation in regard to the CVEs produced under this pilot being pushed to NVD?
    - Why this matters: Stakeholders need to understand what might change for them and have a plan as to how they should respond to those changes. We do not want to create surprises or unexpected technical or procedural problems. NVD currently adds additional information to the CVEs issues by the CVE Team, such as the CPE, CVSS, and CWE information. If these pilot CVEs contain less information (e.g., no description), this could require a lot more work on the part of NVD. Also, some CVEs may not be seen as in scope for NVD. Finally, depending on the criteria for success (e.g. must be usable by all use cases), a clear understanding the expectations could help with the assessment of the pilot results.

7. Could DWF elaborate on the minimum data set (e.g., references) it will produce in its CVEs?
    - Why this matters: Understanding what data DWF will produce may help us pinpoint the right balance of data to serve the broadest range of use cases, once the pilot has been run for a given length of time.

8. What types of documentation do we need from the DWF project? (e.g., scope, products and sources covered, counting standards, what information DWF collects and publishes, rules for becoming a CNA.)
    - Why this matters: Understanding how DWF operates will assist in understanding what changes may need to be made to the CVE program based on the results of the pilot.

9. If DWF is not providing descriptions or references, is the CVE team expected to provide them or are they intended to be published without descriptions? If we are expected to provide descriptions and/or references, should we only do that for what is in scope on the current products list? Do we allow researchers to provide descriptions and/or references?
    - Why this matters: The work of creating viable CVE entries must occur despite the experiment. This helps everyone understand who is responsible for ensuring that is the case. Without clear boundaries and responsibilities, work can be duplicated and there will be conflicts.

10. Is there an end date for the pilot? How often should we meet to evaluate interim results and progress? What is a sufficient amount of time to determine if the pilot should become part of production and continue permanently?
    - Why this matters: An end date will create a point where the EB can evaluate the results of the experiment and decide how to move forward. Without an end date, the pilot could be prematurely shutdown before being given a chance, or it could get stuck in a semi-permanent state and never be fully integrated.

11. What happens when the end date occurs? Are the DWF CVEs removed from the corpus, and what are the criteria by which that decision is made? Should we prepare for a transition plan for the CVEs, regardless of what happens to the pilot program?
    - Why this matters: The Editorial Board should decide if the changes and results are acceptable. If so, the next steps can be planned out for continuing the processes. If the Editorial Board decides the changes and results are not acceptable, plans can be made to remediate any negative impact and changes can be made to future pilots to avoid similar changes and results. Many requesters and vendors could be frustrated if we were to throw out the pilot program CVEs at the end of the pilot program, so we should consider how to transition these CVEs in some form.

12. When the pilot launches, how should we notify the community that it exists, that it is underway, and the process it is following? Are there forums that should be used to communicate this information in addition to the CVE website?
    - Why this matters: The more involvement we have from the CVE community, the more confidence we will have in the results and our understanding of which use cases are being satisfied by the pilot.