The CVE Editorial Board met via teleconference on 5 May 2016. Members of the MITRE CVE Team also attended the call. Board members in attendance were:

- Andy Balinksy, Cisco
- Harold Booth, NIST
- TK Keanini, Cisco
- Kent Landfield, Intel
- Tom Millar, US-CERT
- Kurt Seifried, Red Hat
- Dave Waltermire, NIST

The first item on the agenda was to give an update on the action items from the previous Editorial Board meeting.

MITRE is currently working with their Legal Department regarding Intellectual Property Rights (IPR) over CVE content. MITRE's position is to avoid having a lot of licenses passed downstream to consumers who would then have to maintain compliance with them. MITRE is proposing to update the existing CVE Terms of Use, which states that anyone is allowed to use CVE content and it's free of charge, to cover any contributions to CVE. The intent is to encourage contributions and ensure that the CVE List is available to downstream users. It is important to be clear that MITRE is not in any way asserting IP rights; rather, we are concerned about contributed content that would assert IP rights, which could potentially impact every consumer of that content. The example that triggered this concern was the fact that all DWF data is covered under the Apache license. MITRE took the action to consult with their legal department about allowing for broad, distributed writing in the CVE database, using the Apache license to pull data in, and any IPR implications that may result.

The second action item was the status of standing up Phase 1 of the DWF CNA. For Phase 1, DWF will act as a traditional CNA, which will help to meet the needs of the security researcher community. DWF-issued CVE IDs would all be in the one million CVE ID space. There was a technical implementation meeting on DWF last week. Most of the code has been assembled to import code; some additional modifications still need to be added.

During this Phase 1 period, MITRE would not write CVE descriptions for vulnerabilities with DWF-issued CVE IDs. DWF will assign CVEs, mark them as assigned, and - if the vulnerability is public - mark it as public. From there, the CVEs will be added to the DWF database, which will be as up to date as possible. MITRE will ingest the DWF-issued CVE IDs into the CVE List and mark them as "Reserved." Phase 1 will contain hundreds or thousands of entries with or without descriptions; MITRE is unable to incorporate CVE descriptions written by DWF at this time until legalities such as IPR and licensing are worked out. Once MITRE Legal gives approval to ingest descriptions created by DWF, those descriptions will be included in the CVE List.

Documentation for both Phase 1 and Phase 2 needs to be developed - SLAs, expectations, behaviors, best practices, swim lanes. Items like issuing CVE IDs back-stream to DWF, the initial

DWF assignments of CVEs, and SLAs requiring enough data to create enough of a description will need to be documented. The next step will be to create sub-CNAs to be CNAs for their own products (Phase 2).

The next action item was to set up a coordination call with Intel PSIRT. This meeting is scheduled for May 6, and MITRE will have an update following that.

The next action item is to update documents we want to give to new CNAs, and reconciling those with DWF documents, which is in process. As for implications of the CVE ID block, MITRE foresees no problems with their existing infrastructure.

The last action item is to investigate moving CVEs read/only on GitHub, and this item remains outstanding.

The discussion turned to CVE Scope, the next item on the agenda. CVE needs to start scoping a more focused set of products and sources than in the past. Sources documented in the past were more limited than the scope used in practice. CVE must be a reliable, consistent source of information. Improving CNA processes will help.

The overall goal is for CVE to have a larger scope and to maximize CVE coverage beyond MITRE. The appropriate bodies, such as ISACs (e.g., automotive, aviation), will need to be educated and brought on board to cover vulnerabilities in their products. The long term goal is to have many more CNAs responsible for their own products. The CNAs will work through the CNA rules, and MITRE will be in a CNA oversight role (coordination, documentation, etc.).

Documents and training need to be established to advise CNAs what to do and when to do it. Swim lanes will need to exist so there’s no crossover or as little crossover as possible. A contact list will be provided to identify where and how to refer ID requesters. MITRE will need to establish an outreach program with vendors, particularly large vendors, who are not CNAs.

CVE needs to determine how to address vendors that are not CNAs and do not make vulnerability information public, even when researchers report on vulnerability information concerning their products. For example, researchers publish vulnerabilities that they find in SAP, and they tend not to ask for CVE IDs. SAP does not make vulnerability information public. MITRE web scrapers monitor public vulnerability sources and find these SAP vulnerabilities. MITRE then assigns CVE IDs to them and incorporates them into the CVE List. MITRE has contacted SAP about being a CNA and SAP has not expressed interest. A proposed solution is to send these vendors a notification that MITRE will no longer assign CVE IDs, provide them with a block of CVE IDs, and instruction as to how to assign them. Resources are limited, and if customers are not demanding that CVE support something, then CVE will not provide support for it. If customers start demanding CVE IDs for a certain vendor, then the vendor will need to issue CVE IDs.

MITRE will continue to work off of a defined scope and Products and Sources list and will continue to use these as a filter for what cve-assign covers. Periodic updates are made to the Products and Sources to address changes in the marketplace.

MITRE provides descriptions for all of the CVE IDs it assigns. MITRE uses these descriptions to help determine if a CVE ID has already been assigned to a vulnerability. If the CVE already exists, then the existing CVE is updated with new references and/or details. Other organizations use these descriptions to accelerate their analysis process and to do vulnerability scoring.

DWF will investigate automating the creation of CVE descriptions. DWF will have strictly well-formed data for its entries and various hierarchies for the community. The goal is to attain a point where descriptions can be automatically generated and remain valuable for current usage without denigrating or reducing the quality of looking at CVEs.

Communicating requirements to industry is one way of advancing things, and a community of practice is needed on this subject. MITRE will look into non-government and non-MITRE platforms to stand up a vulnerability reporting community of practice. In the meantime, there will be a large reliance on DWF to get researchers on board and determine what a well-formed request is, what information is required, and what fields are necessary to get an ID.

MITRE posted to the GitHub site current suggested guidelines for a well-formed request and will also send it out to the Editorial Board mailing list for discussion. The DWF documentation will be posted to the Editorial Board list as well so people can start reviewing it and correlating it with the MITRE documentation.

The final discussion revolved around MITRE standing up smaller working groups for the Editorial Board in areas that might be beneficial. It was previously established that a working group will be set up for the structure of the federated CNA program – the process needed, etc. There will also be a working group around the proper way to submit a CVE ID request, with future discussions as to what is well-formed. There also needs to be a swim lane discussion, a vulnerability ontology or taxonomy discussion, and a subgroup for standing up the community of practice on vulnerability reporting.

Action items:

- Expedite DWF pilot with legal (somewhat dependent on DWF's documentation) (MITRE)
- Look at the swim lane document and the Products and Sources list (MITRE)
- Create a mailing list for a vulnerability reporting community of practice (MITRE)
- Put together a list of subgroups for Board discussions (federation, community of practice, swim lanes, and taxonomy) (MITRE)

The next Editorial Board meeting will be held on May 19, 2:00 – 4:00 PM EDT.