The CVE Editorial Board met via teleconference on 02 June 2016. The meeting was focused on CNAs and swim lanes. Members of the MITRE CVE Team also attended the call. Board members in attendance were:

Attendees:
Kent Landfield, Intel
Harold Booth, NIST
Andy Balinsky, Cisco
Scott Lawler, LP3
Art Manion, CERT
Dave Waltermire, NIST

Action items from the previous Editorial Board meeting were reviewed:

- Update the Board charter and distribute out to the Board for discussion and vote (MITRE)
    - The charter has been updated and is undergoing internal MITRE review. It will be sent to the Board for review soon.
- Send out list of working groups to solicit members (MITRE)
    - This is also currently being worked.
- Send an email to the Board to discuss swim lanes and products and sources (MITRE)
    - This has been done and will be discussed today.
- Develop a template for nominating prospective Board members (MITRE)
    - This is in development and will be sent out shortly.
- Look into Google Hangouts as a possibility to replace Skype (MITRE)
    - This is probably not a viable option, because of connection issues due to proxy settings.

The Board raised some concerns regarding DWF using the Apache license for content. Difficulties are being experienced with providing information downstream in the public domain due to having to incorporate the Apache license explicitly.

It was noted that the lawyers at Red Hat and MITRE are in agreement for the new license and are working some details regarding documentation of roles and responsibilities. MITRE legal will have the updated CVE Terms of Use shortly and it will ensure contributions to CVE from outside of MITRE can be published to the CVE List and are easily usable by downstream users.

The discussion turned to CNA status and updates. MITRE is identifying other entities that want to become CNAs. Both vendors and research organizations have contacted MITRE about becoming CNAs, but primarily large companies that sell computer hardware and software products on an international basis.

There were significant discussions around the need for documenting and communicating the rules for being an official CNA and what happens if the rules are not followed. The Board expressed that the rules and requirements for being an official CNA needed to be defined before

new CNAs should be brought on. MITRE will serve as the coordinator and will contact existing CNAs to notify them that things are changing and they will need to understand and follow the new rules. It was noted that other communities (e.g., medical devices, industrial controls) have a need for CVE IDs, but have a different model than the IT community for how they manage their environments. The Board agreed that the new rules would need to account for that and provide the desired end state and give a lot of latitude as to how to do things.

Another aspect that will need to be defined is how those responsibilities are monitored. General consensus is that this also falls to MITRE and that MITRE will serve as a coordinator to ask and track issues. Individual Board members should not reach out to CNAs on behalf of CVE regarding adherence to the rules or for quality statistics.

The discussion turned to defining swim lanes for making CVE ID requests in order to develop the current swim lane descriptions such that a document can be publicly available to the community.

- For specific vendor-related vulnerabilities, and that vendor is a CNA, then the researcher should contact the specific vendor in accordance with their documented CVE ID Request Process.
- ICS-CERT can handle certain industrial control system CVE ID requests in accordance with their process.
- For CERT-CC, CVE IDs are assigned for CERT-CC coordinated incidents; the technology is not as important as the conditions of case (e.g., multiple vendors, when the researcher and the vendor are not getting along, critical infrastructure).
- JPCERT/CC issues CVE IDs for vulnerabilities reported through the "The Information Security Early Warning Partnership" (http://jvn.jp/en/nav/jvn.html).
- MITRE provides coverage for a defined set of products and sources and can also serve as the CNA of last resort, and assigning IDs for products not covered by other CNAs.

The Board also began formalizing the definitions of the CNA categories based on the existing CNAs. These categories might be Product Vendor (e.g., Apple, Cisco), Coordination Center (e.g., ISC-CERT, JPCERT/CC), and root CNAs (DWF-type entities). The categories will be designed to work for any sector, not just IT. The CNA categories will be based on how assignments are done and the organization's scope.

It was noted that one of the challenges in terminology around MITRE is that MITRE serves multiple roles – CNA of last resort, coordinator, publisher of the official CVE list.

Action items:

- Write a draft of CNA requirements based on what was discussed (Art Manion)
- Refine swim lanes document based on discussion and distribute to the Board for review (MITRE)
- Update the CERT-CC swim lane description (Art Manion)

Outstanding Action Items:

- Template for Board nominations (MITRE; in progress)
- Board Charter (MITRE; in progress)

The next Editorial Board meeting will be held on June 16.