CVE Editorial Board Member Roles, Tasks, and Qualifications

Date: March 11, 2015
Document version: 1.4

Roles for CVE Editorial Board Members

Note that some members may have more than one role on the Editorial Board. However, all members have only one primary role.

Implementers provide input and guidance related to issues regarding the creation, design, review, maintenance, and applications of CVE. This role may include content and development engineers working for software vendors, such as individuals who integrate CVE Identifiers into products.

Liaisons represent a significant constituency, related to or affected by CVE. In some cases, a liaison may represent an individual organization. This role may include representatives from software vendors who represent the needs of their company, customers, and partners, such as product managers and product strategists.

Advocates actively support or promote CVE in a highly visible fashion. This role is reserved for respected leaders in the security community who help bring credibility to the CVE Initiative and give CVE a wider reach outside of the security community.

Emeritus members were formerly active and influential in the CVE Initiative. As a result of significant contributions, they maintain an honorary position on the Board.

Minimum Expectations for CVE Editorial Board Members

CVE Editorial Board members must meet the minimum levels of effort consistent with the tasks that they undertake. If a Board member participates in multiple tasks, then the minimum expectations for each individual task may be lowered accordingly.

All members are expected to commit a minimum of 2 hours per month to maintain high-level awareness of ongoing CVE and Editorial Board activities. There may be additional requirements depending on additional tasks.

Participation should be consistent with respect to the specific task. Allowances can be made for extenuating circumstances that temporarily prevent a member from meeting the minimum level of participation.

Tasks for All Members

All members are expected to perform the following tasks:

1. Consultation: This includes participating in Board meetings, or discussion of ad hoc issues related to CVE content or CVE Editorial Board processes such as content decisions, Board membership, or CVE compatibility.
2. Awareness: This includes participating in CVE Editorial Board meetings and/or reading meeting summaries, and regularly reading posts on the CVE Editorial Board mailing lists.

Many members may perform the following tasks:

1. Outreach: Some Board members actively promote CVE and educate the public about CVE, or introduce various contacts to MITRE within the CVE context.
2. Non-CVE activities: Some Board members may participate in activities that are undertaken under the CVE Editorial Board context, but not directly related to CVE.

Estimated Level of Effort

The amount of effort for these tasks may vary widely. Each consultation task usually requires 1 to 10 hours, occasionally more. Such tasks may occur approximately once every 2 months.

Implementer Tasks

In addition to those tasks that are required of all members each implementer should regularly perform one or more of the following tasks:

1. Oversight and Review: Review and comment on new CVE Identifiers, as necessary.
2. Content Provision: Some Board members provide portions of their vulnerability databases to MITRE for conversion into CVE Identifiers, which ensures that CVE content is as complete as possible. Others are actively involved in CVE Identifier reservation. Others may be CVE Numbering Authorities (CNAs), which are authorized to assign CVE Identifiers to security issues before they are publicized.

Expected Level of Effort

Implementers are expected to provide oversight and review on an ad hoc, as needed basis. Those providing content should expect to spend 1 to 5 hours, approximately once every 2 months.

Qualifications for Implementers

1. Implementers should have a minimum of 3 years of experience as a computer security professional (preferably 5 years). Exceptions may be made for individuals who have made noteworthy contributions to the security community.
2. Implementers should be experts in the use or development of one or more of the following technical areas:
   - Vulnerability assessment and related tools
   - Intrusion detection and related tools
   - Incident response or forensics
   - Academic/research topics such as vulnerability or exploit analysis, taxonomies and classification, new security models, or programmer behaviors
   - Related areas
3. Implementers should have strong knowledge about computer security issues in most of the following areas:
   - Concepts such as buffer overflow, SQL injection, open-redirect, cross-site scripting, etc.
   - Commonly exploited vulnerabilities, or related tools
   - Security models in operating systems, protocols, applications, etc.
   - Vulnerability information sources, e.g. advisories, mailing lists, or hacker sites
   - Extensive, real-world operational experience in patch prioritization, vulnerability scanning, policy compliance, and/or threat and incident management

The individual’s knowledge may be broad (e.g., general knowledge of various types of flaws in many different OSes) or deep (e.g., analysis of programming errors in a single OS or programming language).

4. Implementers should be able to effectively identify and communicate technical issues that relate to CVE and their particular area of expertise.
5. Implementers should have a demonstrated commitment to sharing information to enhance research or education, or to improving overall enterprise security, e.g., by active participation in conferences or other forums.

Liaison Tasks

Liaisons should perform one or more of the following tasks, in addition to those tasks that are required of all members:

1. Community Education: Educate the liaison’s own community about CVE, where appropriate.
2. CVE Editorial Board Education: Educate the CVE Editorial Board about the needs and interests for CVE of the liaison's community, particularly relating to patch prioritization, vulnerability scanning, policy compliance, and/or threat and incident management.
3. Other: Undertake other technical tasks and in ad hoc consultation tasks.

Expected Level of Effort

Liaisons are expected to commit approximately 1-2 hours per week to maintain enough high-level knowledge of CVE and CVE Editorial Board activities to effectively educate their constituency, and the Board, on CVE-related issues.

Qualifications for Liaisons

1. Liaisons that represent a constituency beyond an individual organization must be visible and active in the liaison’s constituency community.
2. Liaisons that represent an individual organization must be able to effectively communicate with all other relevant parts of that organization.
3. Liaisons must be familiar with patch prioritization, vulnerability scanning, policy compliance, and/or threat and incident management.
4. Software vendor liaisons must be able to effectively communicate with the vendor's security and product development teams.

Advocate Tasks

Advocates should perform one or more of the following tasks, in addition to those tasks that are required of all members:

1. Endorse CVE: Endorse CVE to constituencies that will benefit from it.
2. Foster Communication: Foster better communication between constituencies.
3. CVE Editorial Board Participation: Participate in CVE Editorial Board activities, especially in decisions related to Board structure and strategic activities.
4. Other: Advocates may undertake integrator or liaison tasks.

Expected Level of Effort

The expected level of effort is variable, but the advocate should participate at least once every 6 months.

Qualifications for Advocates

1. Advocates should be a recognized leader in the security community, as approved by members of the CVE Editorial Board.
2. Advocates must be knowledgeable about patch prioritization, vulnerability scanning, policy compliance, and/or threat and incident management.

Emeritus Tasks

Emeritus members may participate periodically in integrator, liaison, or advisory tasks.

Expected Level of Effort

Emeritus members may participate at will in the CVE Initiative, and are invited and encouraged to do so. However, there is no requirement for Emeritus member participation.

Qualifications for Emeritus

1. Emeritus members must have made significant contributions to the CVE Initiative, as determined by MITRE.

Recognition of Former Members

A person who has left the CVE Editorial Board is recognized in one of the following ways:

1. If the person has qualified for Emeritus status, then the member is identified as Emeritus.
2. If the person did not qualify for Emeritus status, but made clear contributions to CVE as determined by MITRE, then the member is identified as a former contributing member.
3. If the person did not make any measurable contribution to CVE, then the person is not identified as a former member.

CVE Editorial Board Roles for MITRE

The following roles are unique to MITRE:

1. CVE Editorial Board Moderator: The Moderator of the CVE Editorial Board is responsible for the structure of the Board, management of Board mailing lists and meetings, recruitment of new members, and additional Board activities.
2. IP Protection: MITRE is responsible for protecting contributed and transferred intellectual property (IP) and makes non-competitive use of contributed IP, with appropriate licensing and access.
3. Other: MITRE undertakes additional tasks, including CVE content creation, CVE web site maintenance, CVE adoption, and community outreach.

For background discussion on Board Member Roles, Tasks, and Qualifications, refer to archived notes from a meeting held in March 2001, as documented in the summary at http://cve.mitre.org/community/board/archives/2001-03/msg00014.html