# CNA Candidate Process

CVE Numbering Authorities (CNAs) are organizations that distribute CVE IDs to researchers and information technology vendors for inclusion in first-time public announcements of new vulnerabilities. On an as-needed basis, CVE adds CNAs to the CVE community and provides the CNA with a block of CVE IDs annually for the CNA to assign. CNAs are expected to participate in the oversight and administration of CVE ID assignment for products within their scope to satisfy the use cases of the entire set of CVE stakeholders.

## CNA Qualifications

A CNA must be either a major software vendor with a significant user base and an established security advisory capability or an established entity that typically acts as a neutral interface between researchers and vendors. MITRE functions as the primary CNA for CVE.

The CNA must be an established distribution point or source for first-time vulnerability announcements (which may concern their own products). In keeping with the CVE requirement to identify public issues, the CNA must only assign CVE IDs to security issues that will be made public. Finally, it must follow responsible disclosure practices that are accepted by a significant portion of the security community. Responsible disclosure practices reduce the likelihood that duplicate or inaccurate information will be introduced into CVE.

## On-Boarding New CNAs

1. A CNA candidate (referred to as "candidate" from this point forward) is identified.

* A candidate contacts CVE at cve@mitre.org asking for CNA appointment; or
* CVE identifies an entity that may be a good candidate.

1. The Editorial Board reviews the candidate.

* If CVE identified the candidate, CVE consults with the Board to determine if the candidate should be engaged.
* If a candidate initiated the process, the candidate's request will be reviewed by the Board before moving forward. The Board may request additional information or conditions for the candidate, which will be factored in to the rest of the process.

1. CVE engages the candidate and shares general information about CNAs.

* Information will include what a CNA is and expected roles and responsibilities.

1. The candidate assigns a primary and secondary point of contact for initial coordination with CVE and the Board.
2. Anyone acting in a CNA analyst capacity at the candidate's institution will be given training by CVE or by a CNA, which will include:

* Examples and exercises to work through with CVE feedback and instruction;
* Documentation to review and follow; and
* Specific process descriptions.

During this training, an initial block of CVE IDs will be allocated to the candidate for use with their training.

1. The candidate will document how CVE processes will be integrated into their operations.

* CVE will offer documentation describing best practices.
* The candidate's documentation will include how they will process new requests for CVE IDs, internally and externally. If the candidate will process external CVE assignment requests, those specific processes will be documented for public release.
* All documentation will be shared with CVE and may also be shared publicly by the candidate.

1. CVE will review documentation and work with the candidate to address any issues in their processes that may conflict with the established CVE infrastructure.
2. When the candidate meets all other requirements and is prepared to take on the CNA role, CVE and the candidate sign a memo of understanding (MOU) describing each entity's roles and responsibilities.
3. CVE allocates the candidate their yearly block of CVE IDs to assign.
4. The candidate's representatives are added to the CNA operations discussion list. (See below.)
5. The candidate enters operational mode and is now considered a CNA.
6. CVE will update public documentation to include the new CNA and Board member. CVE and the CNA will coordinate public announcements introducing the new CNA.

## Throughout the Candidate Process

CVE and the Board will review and revise general CNA documentation on a yearly basis including:

* CNA qualifications;
* CNA description, roles, and responsibilities;
* CNA training documentation; and
* CNA/CVE MOU.

CVE will perform a quality assurance process for each CNA. This process is described separately. The goal of this process is to ensure CVE IDs are allocated and documented in ways that satisfy the use cases of all of CVE’s stakeholders.

Any changes in a CNA's program, including staff changes or process changes, must be documented and shared with CVE.

## Required Documentation

CVE and the Board will maintain the following documentation.

* Documents describing CNAs and CNA qualifications, roles, and responsibilities
* CVE assignment training documents, including sample processes, examples, and exercises
* CNA quality assurance criteria and performance metrics
* CNA/CVE Memo of Understanding
* CNA roster and points of contact
* Internal process documentation for managing the CNA program

CNAs will maintain the following documentation.

* CVE assignment operations documents

## Goals

CVE satisfies the following goals through the CNA candidate process:

* The candidate understands its roles and responsibilities.
* Individual members of the new CNA's team are able to perform CVE assignment and counting processes.
* Clear communication channels exist between CNAs and CVE.

## Communications

Coordination with the Board occurs over the Editorial Board mailing list.

CVE will maintain a publicly available point of contact (POC) for CNA issues. The specific POC will depend on the current operational practices of CVE, utilizing an email address or a web page as a public contact point, for example.

A new mailing list will be established by the CVE Team for internal discussion of operational issues between CNAs. Members of the list will not be restricted to the individual POCs and can instead include anyone involved with CNA operations. The list will be closed and private (if determined to be appropriate based on Board and sponsor feedback). Board members are also welcome to join this list.

# CNA Roles and Responsibilities

1) The CNA must be either:

(a) A major software vendor with a significant user base and an established security advisory capability, or

(b) An established third party coordinator that typically acts as a neutral interface between researchers, vendors, and/or other parties.

2) The CNA must have an established distribution point for first-time vulnerability disclosures that are freely available to the general public without restrictions.

3) The CNA must only assign CVE-IDs to security issues that will be made public.

4) The CNA must follow coordinated disclosure practices that are accepted by a significant portion of the security community.

5) The CNA must consistently apply documented CVE content decisions (with exceptions made for technical subtleties or incomplete documentation).

6) The CNA must coordinate the exchange of CVE-ID numbers across all parties involved in the disclosure.

7) The CNA must recommend best practices in vulnerability disclosure to both researcher and vendor.

8) The CNA must verify that a reported vulnerability has not already been assigned a CVE-ID.

9) A vendor CNA must clearly advertise its security point of contact.

10) A vendor CNA must include CVE-ID numbers in its own advisories.

11) A vendor CNA can only use their pool of CVE-IDs for vulnerabilities in their own products or area of responsibility.