GCVE-BCP-06 - Requirements and Evaluation Criteria for GCVE Numbering Authorities (GNAs)

GCVE.eu

GCVE.eu

Contents

1 GCVE-BCP-06 - Requirements and Evaluation Criteria for GCVE Numbering Authorities (GNAs)

GCVE.eu

- **Version**: 1.1
- **Status**: Draft (for Public Review
- **Date**: 2026-03-10
- **Authors**: GCVE Working Group
- **BCP ID**: BCP-06

1.1 Introduction and Status Considerations

GCVE BCP-06 aims to define measurable operational expectations for GCVE Numbering Authorities (GNAs). Unlike identifier syntax or synchronization protocol specifications, this document addresses governance models, disclosure philosophies, operational transparency, and data quality characteristics. These dimensions are inherently diverse across the GCVE ecosystem.

GNAs may differ significantly in:

- Disclosure philosophy (coordinated disclosure, partial coordination, immediate full disclosure)
- Review models (automated allocation vs. human-reviewed publication)

- Organizational structure (vendor-operated, research-driven, community-based, independent)
- Resource availability and operational maturity
- Legal and jurisdictional constraints

Because of this diversity, achieving broad consensus on normative requirements is expected to be challenging. BCP-06 attempts to balance:

- Decentralization and autonomy
- Transparency and accountability
- Flexibility and measurable conformance

The objective of this document is not to impose uniform operational behavior, but to define a common framework for describing and evaluating operational characteristics in a machine-readable and publicly verifiable way.

1.1.1 Draft Maturity Expectation

It is anticipated that BCP-06 may remain in Draft or evolving status for an extended period. Operational realities across GNAs will likely change over time, and early adopters may surface edge cases not yet captured in this version.

This document therefore embraces an iterative maturity model:

- Early versions focus primarily on transparency fields.
- Later revisions may refine metrics based on ecosystem feedback.
- Some evaluation criteria may be adjusted as empirical data becomes available.
- Fields may evolve to better reflect real-world operational diversity.

Stability of identifier semantics remains non-negotiable. However, governance and process evaluation criteria are expected to mature over time as the ecosystem stabilizes.

1.1.2 Living Consensus Model

BCP-06 should be understood as:

- A consensus-seeking document rather than a top-down mandate.
- A transparency framework rather than a centralized ranking authority.
- A foundation for ecosystem-driven refinement.

Long-term stability of GCVE depends not on uniformity of GNAs, but on clarity of their operational posture. BCP-06 formalizes that clarity.

Accordingly, implementers and GNAs are encouraged to:

- Provide feedback on feasibility of metrics.
- Report operational edge cases.
- Suggest additional machine-measurable indicators.
- Participate in periodic revision cycles.

The strength of GCVE lies in decentralized accountability. BCP-06 is designed to support that principle even if “full” consensus requires time.

2 Introduction

This document defines the requirements and evaluation criteria for GCVE Numbering Authorities (GNAs) operating within the GCVE ecosystem.

It establishes a standardized framework to assess the extent to which GNAs adhere to the GCVE Best Current Practice (BCP) series, covering:

- Governance
- Allocation quality
- Disclosure processes
- Data interoperability
- Synchronization with the GCVE reference implementation

To promote transparency and consistency, this BCP introduces a standard set of conformance fields to be embedded in the GCVE directory JSON format. These fields enable:

- Automated reporting
- Public visibility of compliance posture
- Third-party ranking and scoring
- Longitudinal evaluation

The objective of this document is to ensure accountability while preserving the decentralized nature of GCVE, support continuous improvement, and strengthen trust in the accuracy and integrity of vulnerability identification across the GCVE network.

3 Design Principles

BCP-06 follows these principles:

1. Decentralization First - No central approval authority.
2. Transparency Over Uniformity - Different operational models are allowed.
3. Machine-Measurable - Boolean or numeric whenever possible.
4. Public Accountability - Conformance data must be public.
5. Continuous Improvement - Metrics allow objective tracking over time.

4 Recognition of Operational Models

GCVE acknowledges that GNAs may operate under different disclosure philosophies and operational constraints.

This BCP does not privilege one model over another but ensures their characteristics are transparently expressed.

Indicative operational profiles include:

Profile Type	Description
Automated Allocator	Issues identifiers automatically with minimal validation
Community Reviewer	Community-driven validation before publication
Vendor Authority	Vendor-operated authoritative disclosure
Research Publisher	Independent research group publishing advisories
Immediate Full Disclosure	Publishes full technical details immediately, without coordinated disclosure delay
Private Publication Only	Allocates identifiers and shares vulnerability data exclusively within a restricted user group named as private GNAs

Immediate Full Disclosure GNAs may:

- Publish exploit details at allocation time
- Not provide embargo handling
- Not engage in coordinated vulnerability disclosure (CVD)

BCP-06 evaluates transparency and stability and not the disclosure philosophy of a GNA.

4.1 Requirement

A GCVE Numbering Authority (GNA) MUST declare and operate under exactly **one operational model** and **one publication visibility model** at any given time.

A single GNA identifier MUST NOT represent multiple operational models simultaneously.

5 Governance Requirements

5.1 Public Disclosure Policy

Requirement:

GNA MUST maintain a publicly accessible disclosure policy describing its operational model.

Evaluation Fields:

- `has_public_disclosure_policy` (boolean)
- `disclosure_policy_url` (string)
- `disclosure_policy_last_updated` (date)

The disclosure policy MUST clearly state whether the GNA:

- Uses Coordinated Vulnerability Disclosure (CVD)
- Supports embargoes
- Operates under immediate full disclosure

5.2 Contact Point for Coordination

Requirement:

GNA MUST provide a stable contact point.

Evaluation Fields:

- `has_security_contact` (boolean)
- `security_contact_type` (enum: email, webform, pgp, other)
- `security_contact_pgp_available` (boolean)

5.3 Organizational Transparency

Recommended:

- Public operator identification
- Defined scope of allocation
- Conflict-of-interest statement (if applicable)

Evaluation Fields:

- `operator_publicly_identified` (boolean)
- `scope_defined` (boolean)
- `conflict_of_interest_statement` (boolean)

6 Disclosure Process Transparency

BCP-06 does not mandate CVD, but requires disclosure transparency.

6.1 Disclosure Model

Evaluation Fields:

- `disclosure_model` (enum: `cvd`, `partial_cvd`, `immediate_full_disclosure`, `automated_publication`, `private_publication`)
- `supports_embargo_process` (boolean)
- `embargo_policy_public` (boolean)
- `average_embargo_duration_days` (integer or null)

As an example, for Immediate Full Disclosure GNAs:

- `disclosure_model` = `immediate_full_disclosure`
- `supports_embargo_process` = false
- `average_embargo_duration_days` = 0

6.2 Review and Allocation Process

Evaluation Fields:

- `human_review_required` (boolean)
- `automated_allocation` (boolean)
- `review_sla_days` (integer or null)

6.2.1 Minimum Transparency Requirements for Private GNAs

Even if vulnerability content is not public, the following MUST be published:

- GNA identity

- Scope of allocation
- Disclosure model
- Publication visibility model
- Synchronization endpoint availability
- Identifier status (published, reserved, rejected)

Private GNAs MUST NOT obscure the existence of allocated identifiers.

The GCVE ecosystem depends on global identifier uniqueness, even when vulnerability details are restricted.

7 Allocation Quality Criteria

These metrics evaluate identifier hygiene and reference stability.

7.1 Identifier Stability

Requirements:

- Identifiers MUST NOT be reused. Identifier reuse occurs when a previously assigned GCVE ID is used again for a different vulnerability record after deletion, withdrawal, or revocation.
- Identifiers MUST NOT be reassigned. Identifier reassignment occurs when an existing GCVE ID is modified to refer to a completely different vulnerability than originally described.

Evaluation Fields:

- `identifier_reuse_detected` (boolean)
- `identifier_reassignment_detected` (boolean)

7.2 Reference Stability

GNAs SHOULD maintain stable references (permalinks, commit hashes, content-addressable URLs).

Evaluation Fields:

- `uses_permalinks` (boolean)
- `reference_http_200_ratio` (float 0.0–1.0)
- `reference_http_404_ratio` (float 0.0–1.0)

These ratios enable automated link integrity scoring.

7.3 (TO REVIEW) Data Completeness Metrics

Evaluation Fields:

- average_description_length (integer)
- has_cwe_classification (boolean)
- has_cvss_score (boolean)
- has_epss_score (boolean)
- has_vendor_acknowledgement (boolean)
- average_fields_per_record (integer)

BCP-06 does not require all enrichment fields but requires transparency.

8 Interoperability Requirements

GNAs MUST publish data in a machine-readable format.

8.1 Structured Output

Evaluation Fields:

- provides_machine_readable_feed (boolean)
- feed_format (array: json, ndjson, rss, other)
- schema_version_declared (boolean)

8.2 (TO REVIEW) Taxonomy and Standards Usage

Evaluation Fields:

- uses_cwe (boolean)
- uses_cvss (boolean)
- uses_openvex (boolean)
- uses_ossf_schema (boolean)

9 GCVE Synchronization Requirements

Participating GNAs MUST support synchronization with the GCVE reference implementation.

9.1 Sync Endpoint

Evaluation Fields:

- `provides_sync_endpoint` (boolean)
- `sync_endpoint_url` (string)
- `sync_protocol_version` (string)
- `last_successful_sync` (timestamp)

9.2 Sync Reliability Metrics

Evaluation Fields:

- `sync_uptime_ratio_30d` (float 0.0–1.0)
- `average_sync_latency_seconds` (integer)

10 Conformance JSON Publication

Each GNA MUST provide or authorize publication of a machine-readable conformance JSON document.

The JSON MUST:

- Be publicly accessible
- Be licensed under an open data/open source license
- Be versioned
- Be updated at least every 90 days
- Reflect factual operational characteristics

11 Example GNA Conformance JSON

```json
{
  "gcve_bcp_version": "BCP-06-1.0",
  "gna_id": "65535",
  "last_updated": "2026-02-12",

  "governance": {
    "has_public_disclosure_policy": true,
    "disclosure_policy_url": "https://research.example/disclosure-policy",
    "disclosure_policy_last_updated": "2026-01-01",
    "has_security_contact": true,
    "security_contact_type": "email",
    "security_contact_pgp_available": true,
    "operator_publicly_identified": true,
    "scope_defined": true,
    "conflict_of_interest_statement": false
  },

  "disclosure_process": {
    "disclosure_model": "immediate_full_disclosure",
    "supports_embargo_process": false,
    "embargo_policy_public": false,
    "average_embargo_duration_days": 0,
    "human_review_required": true,
    "automated_allocation": false,
    "review_sla_days": 2
  },

  "allocation_quality": {
    "identifier_reuse_detected": false,
    "identifier_reassignment_detected": false,
    "uses_permalinks": true,
    "reference_http_200_ratio": 0.98,
    "reference_http_404_ratio": 0.01,
    "average_description_length": 850,
    "has_cwe_classification": true,
    "has_cvss_score": true,
    "has_epss_score": false,
    "has_vendor_acknowledgement": false,
    "average_fields_per_record": 14
  },
```

```
41
42    "interoperability": {
43      "provides_machine_readable_feed": true,
44      "feed_format": ["json"],
45      "schema_version_declared": true,
46      "uses_cwe": true,
47      "uses_cvss": true,
48      "uses_openvex": false,
49      "uses_ossf_schema": false
50    },
51
52    "synchronization": {
53      "provides_sync_endpoint": true,
54      "sync_endpoint_url": "https://research.example/gcve-sync",
55      "sync_protocol_version": "1.0",
56      "last_successful_sync": "2026-02-11T14:10:00Z",
57      "sync_uptime_ratio_30d": 0.997,
58      "average_sync_latency_seconds": 2
59    },
60
61    "evaluation_metadata": {
62      "evaluation_version": "1.0",
63      "last_evaluated": "2026-02-12",
64      "overall_score": 82
65    }
66  }
```

12 Conformance Philosophy

BCP-06 does not judge disclosure ideology.

It evaluates:

- Stability
- Transparency
- Interoperability
- Operational reliability

A GNA practicing immediate full disclosure can be fully conformant if:

- Its policy is explicit,
- Its identifiers are stable,
- Its data is machine-consumable,
- Its synchronization is reliable.

Transparency is mandatory. Uniformity is not.

13 Acknowledgements

13.1 BCP-07 Coordinators

- Cédric Bonhomme, CIRCL
- Alexandre Dulaunoy, CIRCL

13.2 Contributions

The GCVE initiative gratefully acknowledges the substantial contributions from the following individuals via public review:

- Andras Iklody, MISP Project