Frontier AI Researcher CVE Numbering Authorities (CNAs) Pilot

Targeted at flagship AI organizations seeking CNA researcher role

Frontier AI companies may discover vulnerabilities at a scale, speed, and breadth that existing CVE Numbering Authority (CNA) processes were not designed to absorb. A pilot "AI Researcher CNA" role would help the CVE™ Program capture the benefits of AI-enabled vulnerability discovery capabilities while ensuring that resulting CVE Records are accurate, coordinated, actionable, and sustainable for the ecosystem.

This pilot supplements and does not replace the CNA Operational Rules; participating organizations remain responsible for complying with all applicable CNA requirements. The pilot is intended to focus AI-enabled vulnerability research on frontier labs' products and applications that have achieved meaningful adoption, deployment, or ecosystem significance. Candidate participants should demonstrate sufficient real-world use or stakeholder impact to justify CVE Program attention.

The pilot will operate for an initial six-month evaluation period and will conclude with a formal review of its outcomes, risks, operational burden, and value to CVE consumers. Based on that review, the CVE Program may continue, modify, expand, extend, or end the pilot.

Minimum Operating Requirements for Frontier "AI Researcher" CNA Scope

Validation and Record Quality	Provide reproducible evidence; human validation; severity validation where practical; complete Problem Type/CWE mapping; and identify the product by referring to a repository or download. Provide the most consumable information about affected versions, such as ranges of released versions.
Scope Reconciliation and Deconfliction	Build scope checks into the testing and intake workflow before CVE ID assignment. The Frontier AI Researcher CNA must follow these three requirements: 1. Do not assign a CVE ID if the product is from a Supplier CNA listed on the CVE Program List of Partners page, or the specific Supplier is directly listed on that page in the context of a different CNA, e.g., CERT-VDE; 2. Do not immediately assign a CVE ID if the reporting or security policy for the product states that a different CNA is used. Instead, work with that CNA unless impossible because of restrictive Terms and Conditions; 3. When contacting the Supplier of the vulnerable product, state that the Supplier can choose to assign a CVE ID and publish a corresponding CVE Record through a CNA of their choice. For any non-CNA Supplier, the Frontier AI Researcher CNA can assign and publish after 72 hours if no other CNA has done so. Check for duplicate or overlapping findings, and coordinate with the Root when scope is ambiguous, disputed, or likely to affect other CNA activity.

Coordinated Disclosure	Maintain a documented CVD process for Medium and High vulnerabilities; notify suppliers or maintainers before public disclosure; minimize avoidable zero-day exposure.
Remediation Value	Include a proposed fix, mitigation, or downstream remediation path when feasible unless the supplier or maintainer has stated that proposed fixes are unwelcome. Provide support for reasonable supplier questions about alternative-fixes (e.g., Can I instead guard against a much broader class of invalid input?)
Consumer Needs	Use AI capabilities to assess exploitability conditions, likely deployment exposure, available compensating controls, and whether the issue is likely to matter in real-world configurations. If there is no technical barrier to an installation allowing reachability by untrusted input, but such an installation is unsupported or lacks meaningful real-world security relevance, then do not assign.
Program Coordination	Participate in CVE Program Researcher Working Group and related activities; respond to community requests to improve CVE Records; support deduplication, assignment coordination, and disclosure pacing.
Public Disclosures	Any public vulnerability disclosure that meets CVE Program assignment criteria should receive a CVE ID and published CVE Record regardless of severity level.

Recommendations to Increase Value for CVE Consumers

Document Attack and Deployment Conditions	Capture relevant configurations, exposure assumptions, authentication requirements, and deployment dependencies in the CVE Record where available, potentially in configurations or metrics/scenarios.
Provide SSVC Analysis where Practical [1]	Use the LLM to perform, or attempt to perform, SSVC analysis so consumers have additional decision-support context beyond CVSS, especially when CVE volume increases rapidly.
Improve Remediation Guidance	Use the LLM to propose fixes, evaluate alternative fixes, identify mitigations, and describe compensating controls for consumers who cannot immediately update.
Prioritize High-Value Testing	Select products based on stakeholder and consumer impact, including critical software (as designated by EO 14028), broadly deployed products, unresponsive suppliers, products without Supplier CNA coverage, discontinued bug bounty areas, and technologies with prior severe impact.

[1] SSVC is not currently a data element commonly provided by CNAs, but it may be valuable where consumers are facing a rapidly increasing volume of CVE Records.

Candidate LLM Prompts to Potentially Improve CVE Record Consumer Value

1. Although this product can be deployed in an environment with an attack surface allowing the described attack by untrusted parties, is such an environment guaranteed or even likely?" and its corollary:
2. If untrusted data can reach the corner case that you found, is it also possible for untrusted data to have many other, more obvious but less severe consequences?
3. What are other solution paths beyond changing the code?
4. Can consumers add other controls in their environment or change the configuration?
5. Is the underlying problem that the functionality should not have been exposed in the default configuration?

These types of explorations will provide better information about real-world relevance while also offering options to consumers who cannot immediately update.