Carnegie Mellon University
Software Engineering Institute

COORDINATED VULNERABILITY DISCLOSURE APPLICATION PROGRAMMING INTERFACE PROCEDURE

Brad Runyon
Eric Hatleback
Allen Householder
Art Manion
Vijay Sarvelpalli
Timur Snoke
Jonathan Spring
Laurie Tyzenhaus
Charles Yarbrough

May 2022

Purpose

This white paper provides a set of user stories intended to guide the development of a technical protocol and SPI for Coordinated Vulnerability Disclosure (CVD). These user stories reflect internal discussions with the CERT/CC based on our own experiences in developing and using the VINCE platform, as well as our ongoing CVD practice.

Scope

This document is designed to create the user story the CERT/CC team could imagine. The user stories are expected to be utilized by the team to better understand, create, and implement a CVD Protocol. In addition, the CERT/CC believes these use cases can be useful for any enterprise designing or implementing their own CVD policies, processes, and procedures.

Definitions and Abbreviations

Definitions

CVD Case The unit of work for the overall CVD process for a specific vulnerability spanning the individual CVD Case Participants and their respective report handling processes.

Vulnerability Report The unit of work which contains information about a vulnerability, created by a *Finder* or *Reporte*r and sent to a *Vendor* or *Coordinator*.[1]

CVD Case Participant Finder, Reporter, Vendor, Deployer or Coordinator as defined in the *CERT Guide to Coordinated Vulnerability Disclosure* (a.k.a. "the CVD Guide") [1]. In the context of the use case stories a *Participant* may be in any CVD role.

Throughout this document, we will be referring to the CVD Roles from the *CERT Guide to Coordinated Vulnerability Disclosure [1,2].*

Finder (Discoverer) the individual or organization that identifies the vulnerability

Reporter the individual or organization that notifies the vendor of the vulnerability

Vendor the individual or organization that created or maintains the product that is vulnerable

Deployer the individual or organization that must deploy a patch or take other remediation action

Coordinator an individual or organization that facilitates the coordinated response process

Our *Deployer* role is synonymous with the *User* role in ISO/IEC 29147:2018 and ISO/IEC30111:2019 [3, 4], while the other roles are consistently named.

CVD Phases are the phases which a CVD process may use to track and identify what work needs to be completed to move to the next phase. The phases include:

- **Discovery** – A researcher (not necessarily an academic one) discovers a vulnerability by using one of numerous tools and processes.
- **Reporting** – A researcher submits a vulnerability report to a software or product vendor, or a third-party coordinator if necessary.
- **Validation and Triage** – The analyst validates the report to ensure accuracy before action can be taken and prioritizes reports relative to others.
- **Remediation** – A remediation plan (ideally a software patch but could also be other mechanisms) is developed and tested.
- **Public Awareness** – The vulnerability and its remediation plan is disclosed to the public.
- **Deployment** – The remediation is applied to deployed systems.

MetaCoord is short for Metacoordination, which refers to the support of tools and operational processes such as those listed here:

- **Policy:** A participant may have their own CVD policies and procedures, or they may follow a Vendor's or Coordinator's policies. CVD policies should be public to allow all potential participants to know what the policies are for working with you/your company/organization.
- **Community** (finder/reporter, technical affinity): Vendors, suppliers and customers have a clear relationship. Often a vulnerability in one supplier affects multiple Vendors.
- **Monitoring** (including IR): Monitoring should include awareness of what is happening in the Vendor's company (Incident Response, CSIRT and PSIRT activities) and what is being discussed on social media platforms. Participants that wish to stay informed of new vulnerabilities and areas of interest, may identify a potential vulnerability in their own product.

- **OpSec**: Operational Security is focused on the tools necessary to enforce the embargo while allowing secured or encrypted communications among the participants. All information related to the CVD case should be stored securely.
- **Infrastructure**: The tools which provide the secured or encrypted channel for communication, provide, and support unique CVD case numbers, or implement the authentication/authorization in support of the CVD activities.

Abbreviations

CVD	Coordinated Vulnerability Disclosure
VDP	Vulnerability Disclosure Program
IR	Incident Response
OpSec	Operations Security
MetaCoord	Metacoordination

Use Cases

Using the terms above, the CERT/CC has developed the following user stories to identify the participants, CVD phases and Meta Coordination tools and functions to support each story.

As a Participant

User Story **CVD-API-003-2**
As a Participant I want to receive vulnerability reports that I have submitted through a platform so that I can participate and track coordination efforts
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting
MetaCoord:

User Story **CVD-API-004-3**
As a Participant I want to Discover others' policies
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting
MetaCoord: Policy

User Story **CVD-API-005-15**
As a Participant I want to provide information about my bug bounty program to entice reporters to use it.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases': Reporting
MetaCoord: Policy and Community (finder/reporter, tech affinity)

User Story **CVD-API-006-3.1**
As a Participant I want to parse/evaluate Policies
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting
MetaCoord: Policy

User Story **CVD-API-007-3.2**
As a Participant I want to optimize all the policies involved
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other

CVD Phases: Reporting
MetaCoord: Policy

User Story **CVD-API-008-3.3-3.6**
As a Participant I want decide if I will/can engage *throw a flag if policy trouble detected* *warn participant and need to invoke other channels/humans* *want to post/publish/advertise my policy*
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting
MetaCoord: Policy

User Story **CVD-API-009-9**
As a Participant I want to Publish/share/advertise embargo dates, have hard and absolute limits, have a default/starting point, be able to extend, and propose and accept, stop when all accepts *have a default/starting point* *be able to extend* *propose and accept* *stop when all accepts*
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting
MetaCoord: Policy and Community (finder/reporter, tech affinity)

User Story **CVD-API-010-16**
As a Participant, I want to report a (new) vulnerability
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting
MetaCoord: None

User Story **CVD-API-011-17**
As a Participant I want to Add a participant? (de-duplicate)
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other

CVD Phases: Reporting, Analysis and Remediation
MetaCoord: Community (finder/reporter, tech affinity)

User Story **CVD-API-012-18**
As a Participant, I want to negotiate embargo/disclosure schedules, modify/renegotiate then, and know when others have published
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting, Validation and Prioritization, Analysis and Remediation and Public Awareness
MetaCoord: Policy

User Story **CVD-API-043-21**
As a participant, I want notify others of my intent (date) to publish.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Public Awareness
MetaCoord: None

User Story **CVD-API-044-21.1**
As a participant, I want limited/ACK of vulnerability/and have full/proper advisory
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Public Awareness
MetaCoord: None

User Story **CVD-API-013-24**
As a Participant, I want to share my draft publication with others
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Public Awareness
MetaCoord: None

User Story **CVD-API-014-25**
As a Participant, I become aware of the existence of public exploit PoC and want to tell others
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Validation and Prioritization, and Public Awareness
MetaCoord: Monitoring (including IR)

User Story **CVD-API-016-26**
As a Participant, I become aware of exploitation in the wild of public, exploit PoC and want to tell others
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Validation and Prioritization, and Public Awareness
MetaCoord: Monitoring (including IR)

User Story **CVD-API-017-27**
As a Participant, I want to publish a vulnerability (external to protocol)
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Public Awareness
MetaCoord: None

User Story **CVD-API-019-28**
As a participant, I want to share/publish/advertise my policy including language, locale, national/regional/localness to make sure that we have a common frame of reference or context that sets expectations on the CVD process and its communications.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting
MetaCoord: Policy and Community (finder/reporter, tech affinity)

User Story **CVD-API-045-29**
As a participant, I want to share/publish/advertise the scope (e.g., products, version ranges, sites/domains) of my CVD capability.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting
MetaCoord: Policy and Community (finder/reporter, tech affinity)

User Story **CVD-API-022-33**
As a participant, I want to constrain whom I communicate with because I want to enforce an embargo and communicate only with those who have a need to know.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Discovery, Reporting, Validation and Prioritization, Analysis and Remediation
MetaCoord: Community (finder/reporter, tech affinity) and OpSec

User Story **CVD-API-123-34**

As a Participant I want to Address participants constraints, e.g., entity lists
Roles: Finder, Reporter. Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting
MetaCoord: Community

User Story **CVD-API-124-35**
As a Participant I want to Address participants constraints, e.g., e As a vendor or coordinator, I want others to find my information and reporting intake (duplicate of X)
Roles: Finder, Reporter. Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting
MetaCoord: Policy and Community (finder/reporter)

User Story **CVD-API-048-37**
I want to discover and use/map to a global/shared case ID (might just be a GUID assigned at first notification, CVE is a partial example, vxref).
Roles: Finder. Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Validation and Prioritization, Analysis and Remediation, and Public Awareness
MetaCoord: Infrastructure

User Story **CVD-API-052-53**
I want to use my global/federated user ID to interact with other participants
Roles: Finder. Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Discovery, Reporting, Validation and Prioritization, Analysis and Remediation and Public Awareness
MetaCoord: OpSec, and Infrastructure

User Story **CVD-API-053-54**
I want to have confidence in the identity and group membership of others (and be willing and able to use others' groups)
Roles: Finder. Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting
MetaCoord: Community (finder/reporter), OpSec, and Infrastructure

User Story **CVD-API-028-71**

As a participant I want to add (declare and notify others) new participants to a case
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Discovery, Reporting, Validation and Prioritization, and Analysis and Remediation
MetaCoord: Policy, Community (finder/reporter), Infrastructure

User Story **CVD-API-028-73**
As a participant I want to propose new participants to a case
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting, Validation and Prioritization, and Analysis and Remediation
MetaCoord: Policy, Community (finder/reporter), Infrastructure

User Story **CVD-API-028-74**
As a participant I want to vote/accept new participants to a case
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Validation and Prioritization, and Analysis and Remediation
MetaCoord: Policy, Community (finder/reporter), Infrastructure

User Story **CVD-API-100-75**
As a Participant, I want to state that I paid or received a bounty.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Public Awareness
MetaCoord: None

User Story **CVD-API-101-76**
As a Participant, I want to ask if another participant paid a reporter/finder.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Public Awareness
MetaCoord: None

User Story **CVD-API-102-77**
As a Participant, I want to ask a reporter if they were paid.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other

CVD Phases: Public Awareness
MetaCoord: None

User Story **CVD-API-103-78**
As a Participant, I want to share a draft advisory with others
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting, Validation and Prioritization, Analysis and Remediation
MetaCoord: Policy and Infrastructure

User Story **CVD-API-104-79**
As a Participant, I want to share a draft advisory with others and request feedback (including status)
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting, Validation and Prioritization, Analysis and Remediation
MetaCoord: Policy and Infrastructure

User Story **CVD-API-105-81**
As a Participant, I want to request an advisory (draft) from a participant.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Validation and Prioritization, Analysis and Remediation
MetaCoord: Policy and Infrastructure

User Story **CVD-API-106-82**
As a Participant, I want to request someone else's (vendor) status so I can note changes in other status.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting, Validation and Prioritization, Analysis and Remediation
MetaCoord: Policy and Community (finder/reporter)

User Story **CVD-API-107-83**
As a Participant, I want to state my status, so others are aware of it.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other

CVD Phases: Reporting, Validation and Prioritization, Analysis and Remediation, and Deployment
MetaCoord: None

User Story **CVD-API-108-84**
As a Participant, I want to include a non-vendor role participant in a case.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Validation and Prioritization, Analysis and Remediation, and Public Awareness
MetaCoord: Community (finder/reporter)

User Story **CVD-API-109-88**
As a Participant, I want to include the Government (some/any part, could include regulator groups so that they may participate in the case
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Analysis and Remediation, Public Awareness, and Deployment
MetaCoord: Policy, Community (finder/reporter) and Monitoring (including IR)

User Story **CVD-API-128-89**
As a Participant, I want to include the industry/trade groups so that they may participate in the case
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Analysis and Remediation, and Public Awareness
MetaCoord: Policy, Community (finder/reporter) and Monitoring (including IR)

User Story **CVD-API-110-90,91,92**
As a Participant, I want to stop participating in the case and inform others that I am no longer participating. and no longer will receive or reply to forwarded queries.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting, Validation and Prioritization, Analysis and Remediation, Public Awareness, Deployment
MetaCoord: Community (finder/reporter, tech affinity)

User Story **CVD-API-111-93**

As a Participant, I want to tell others that I published so that they can know about the vulnerability and the mitigation or remediation.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Public Awareness
MetaCoord: Community (finder/reporter)

User Story **CVD-API-112-94**
As a Participant, I want to convey how information I provide can be used so that others can apply the mitigation or remediation correctly.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting, Validation and Prioritization, Analysis and Remediation, Public Awareness, and Deployment
MetaCoord: OpSec

User Story **CVD-API-113-95**
As a Participant, I want to convey how information I provide can be used while obeying the TLP restrictions that others can apply the mitigation or remediation correctly.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting, Validation and Prioritization, Analysis and Remediation, Public Awareness, and Deployment
MetaCoord: Policy, OpSec and Infrastructure

User Story **CVD-API-114-96,97**
As a Participant, regarding the handling of restricted information, I want to convey what Restricted information or degree of restriction I will accept so that I won't be accused of mishandling restricted information. TLP restricted information or degree of restriction I will accept so that I won't be accused of mishandling TLP restricted information.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting
MetaCoord: Policy, Community (finder/reporter), OpSec, and Infrastructure

User Story **CVD-API-029-98**
As a Participant, I want to keep track of events and timelines so that I have a complete report and don't miss a deadline.

Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting, Validation and Prioritization, Analysis and Remediation, Public Awareness and Deployment
MetaCoord: Monitoring (including IR) and Infrastructure

User Story **CVD-API-030-99**
As a Participant, I want to see response times/states of other participants so that I can be prepared for the next state in the CVD process.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting, Validation and Prioritization, Analysis and Remediation, Public Awareness, and Deployment
MetaCoord: Monitoring (including IR) and Infrastructure

User Story **CVD-API-031-102**
As a Participant, I want to be able to ask further questions about a report, to ensure I fully understand the vulnerability and mitigation or remediation options.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting, Validation and Prioritization, Analysis and Remediation, Public Awareness, and Deployment
MetaCoord: Infrastructure

User Story **CVD-API-125-105**
As a Participant, other, I want to publicly disclose sooner than others but minimize their (the other's) exposure/risk.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Public Awareness
MetaCoord: Policy, and Monitoring (including IR)

User Story **CVD-API-116-122**
As a Participant, I want to communicate with all participants associated with this CVD.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Public Awareness
MetaCoord: Infrastructure

User Story **CVD-API-117-106**
As a Participant, I want to communicate important public state change message/information with all participants.

Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Validation and Prioritization, and Analysis and Remediation
MetaCoord: Monitoring (including IR) and Infrastructure.

User Story **CVD-API-118-123**
As a Participant, I want to communicate with non-vendor participants, primarily other defenders, providers, CSIRTs, regulators, etc., important information.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting
MetaCoord: Policy and Community (finder/reporter)

User Story **CVD-API-119-108**
As a Participant, I want to contribute to the creation, modification, and publication of an advisory.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Public Awareness
MetaCoord: Infrastructure

User Story **CVD-API-120-111**
As a Participant, I will prioritize my response to requests for information or action so that I contribute to a rick-minimizing CVD process and outcome.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Validation and Prioritization
MetaCoord: Monitoring (including IR)

User Story **CVD-API-121-112**
As a Participant, I want to share and receive information I can use to prioritize my work regarding the vulnerability report.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting, Validation and Prioritization
MetaCoord: Monitoring (including IR)

User Story **CVD-API-122-113**
As a Participant, I want to avoid missteps by maintaining knowledge of the state of the case and what options are available.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other

CVD Phases: Discovery, Reporting, Validation and Prioritization, Analysis and Remediation, Public Awareness, Deployment
MetaCoord: Policy, Monitoring (including IR), and Infrastructure

User Story **CVD-API-062-114,115,116**
As a Participant, I want/need a mechanism which will Assure me of the authentication and verify integrity of messages; Ensure the appropriate level of authentication of all participants; Ensure the confidential transport and storage of information.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: No Phases
MetaCoord: OpSec and Infrastructure

User Story **CVD-API-063-117, 117.1**
As a Participant, I want to know who else is participating in a case to Avoiding disclosure outside of the embargo group; Ensure the participant list is complete.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Discovery, Reporting, Validation and Prioritization, Analysis and Remediation, Public Awareness, Deployment
MetaCoord: Community (finder/reporter, tech affinity), OpSec and Infrastructure

User Story **CVD-API-064-118,119,120**
As a Participant, I concerned about my reputation and the reputation of other participants. Assurances may be received by: Assessing the reputation of others so that I can decide to engage again; Creating a record or log of my trust in and the reputation of others so I can decide to engage again; By providing evidence of and documenting my reputation to others so they can decide to engage with me.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting
MetaCoord: Community (finder/reporter, tech affinity), OpSec and Infrastructure

User Story **CVD-API-065-121**
As a Participant, I want to create, define, and organize my own groups of other participants so that I can communicate successfully, participate fully and understand their requirements.
Roles: Finder, Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting
MetaCoord: Community (finder/reporter, tech affinity), OpSec and Infrastructure

As a Finder

User Story **CVD-API-037-1**
As a Finder *I want to discover how to report a vulnerability* so that I can alert the affected vendors
Roles: Finder
CVD Phases: Reporting
MetaCoord: Policy and Community (finder/reporter)

As a Reporter

User Story **CVD-API-061-110**
As a Reporter *I want to be rewarded with a bounty*
Roles: Finder
CVD Phases: Reporting
MetaCoord: Policy and Community (finder/reporter)

As a Coordinator

User Story **CVD-API-039-33.3**
As a Coordinator, I want to constrain whom I communicate with to work within an embargo and communicate only with those who have a need to know.
Roles:
CVD Phases: Reporting, Validation and Prioritization, and Analysis and Remediation
MetaCoord: None

User Story **CVD-API-040-103**
As a coordinator, I want to drive better (shorter?) embargo timelines, to ensure they are feasible.
Roles: Coordinator
CVD Phases: Public Awareness
MetaCoord: Policy

User Story **CVD-API-041-104**
As a coordinator, I want to collect and optimize embargo timelines of all participants (probably duplicate of above) to ensure the timelines are feasible.
Roles: Coordinator
CVD Phases: Public Awareness,
MetaCoord: Policy

As a Finder / Reporter / Coordinator

User Story **CVD-API-066 -125**
As a Coordinator I want to validate the report received from Reporter or Finder before deciding to begin CVD for the potential case.
Roles: Coordinator, Finder, Coordinator
CVD Phases: Reporting, and Validation and Prioritization
MetaCoord: none

User Story **CVD-API-127-126**
As a Coordinator I want to collect artifacts such as PoC exploit (Proof-of-Concept), code control flow analysis (static or dynamic) that can enable our validation of the vulnerability being reported.
Roles: Coordinator
CVD Phases: Reporting, and Validation and Prioritization
MetaCoord:

User Story **CVD-API-038-33.1**
As a Finder/Reporter, I want to constrain whom I communicate with because I want to maintain my anonymity.
Roles: Finder, Reporter

CVD Phases: Reporting, and Analysis and Remediation
MetaCoord: none

As a Vendor / Deployer

User Story **CVD-API-046-33.2**
As a Vendor/Deployer, I want to constrain whom I communicate with until a patch or mitigation has been published and released.
Roles: Vendor, Deployer
CVD Phases: Validation and Prioritization, and Analysis and Remediation
MetaCoord: none

As a Reporter / Vendor / Coordinator / Other

User Story **CVD-API-050-46**
As a Reporter, Vendor, Coordinator, Other, I want to ask participant A if participant D is in a case (Operator may decide/policy, may be based on whether C and D are in the same case) "A" may or may not answer, that is their policy (participant may decide/policy, may be based on whether C and D are in the same case)
Roles: Reporter, Vendor, Coordinator, Other
CVD Phases: Analysis and Remediation
MetaCoord: Policy, and Community (finder/reporter, tech affinity)

As a Finder / Reporter / Deployer / Coordinator / Other

User Story **CVD-API-059-107**
I want to publish vulnerability advisories (As a non-vendor participant I want to be informed of CVD to perform activities like risk assessment, mitigation, verify mitigation, not be surprised, prepare messaging, etc.)
Roles: Finder. Reporter, Deployer, Coordinator, Other
CVD Phases: Reporting
MetaCoord: Policy and Community (finder/reporter, tech affinity)

As a Vendor / Coordinator / Other

User Story **CVD-API-047-36**

As a vendor, coordinator or other, I want to assign my own ID to a case.
Roles: Vendor. Coordinator, Other
CVD Phases: Reporting
MetaCoord: Infrastructure

As a Vendor / Coordinator

User Story **CVD-API-057 -57**
As a vendor or coordinator, I want to receive vulnerability reports
Roles: Vendor. Coordinator
CVD Phases: Reporting
MetaCoord:

As a Coordinator / Other

User Story **CVD-API-115-100**
As an Other, (a VDP operator), I want the CVD protocol to also support VDP
Roles: Coordinator, Other
CVD Phases: Reporting, Validation and Prioritization, Analysis and Remediation, Public Awareness, Deployment
MetaCoord: Policy, Community (finder/reporter), Monitoring (including IR), OpSec, and Infrastructure

As a Finder / Reporter / Vendor / Coordinator / Other

User Story **CVD-API-049-39**
I want to get from another participant a list of cases I am involved in with them unicast, multicast, broadcast use/require a shared vul ID space / cross reference? aliases/vxref equals? shared record/ledger? Search/filter?
Roles: Finder. Reporter, Vendor, Coordinator, Other

CVD Phases: Discovery, Reporting, Validation and Prioritization, Analysis and Remediation, Public Awareness, Deployment
MetaCoord: Infrastructure

User Story **CVD-API-039-49**
I want to request/state that I do not want others to know I am in a case Participant still gets to decide their policy Covers researcher asking for anonymity Vendor can ask not to be listed and operator can disagree/still list
Roles: Finder. Reporter, Vendor, Coordinator, Other
CVD Phases: Discovery, Reporting, Validation and Prioritization, Analysis and Remediation, Public Awareness, Deployment
MetaCoord: Policy, and Infrastructure

As a Vendor

User Story **CVD-API-060-109**
I want to reward the reporter by paying a bounty.
Roles: Vendor, Reporter
CVD Phases: Public Awareness
MetaCoord: None

As a Reporter / Vendor / Deployer / Coordinator / Other

User Story **CVD-API-057-57**
I want to ask questions and generally communicate with another case participant
Roles: Reporter, Vendor. Deployer. Coordinator. Other
CVD Phases: Reporting
MetaCoord: None

User Story **CVD-API-024-63**
As a Reporter, Vendor, Deployer, Coordinator, or Other, I want to communicate in a common case channel

Roles: Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting, Validation and Prioritization, Analysis and Remediation
MetaCoord: Infrastructure

User Story **CVD-API-025-64**
As a Reporter, Vendor, Deployer, Coordinator, or Other I want to communicate with selected case participants
Roles: Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting, Validation and Prioritization, Analysis and Remediation
MetaCoord: Infrastructure

User Story **CVD-API-026-65**
As a Reporter, Vendor, Deployer, Coordinator, or Other, I want to produce a shared, verified public record of case activity
Roles: Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Reporting, Validation and Prioritization, Analysis and Remediation
MetaCoord: Policy, OpSec and Infrastructure

User Story **CVD-API-027-66-67**
As a Reporter, Vendor, Deployer, Coordinator, or Other I (we) (might) want the case to have a leader (global case owner)
Roles: Reporter, Vendor, Deployer, Coordinator, Other
CVD Phases: Validation and Prioritization, and Analysis and Remediation
MetaCoord: Policy and Infrastructure

Propose a leader, optionally offer self, step down (see d)
vote/accept
Announce case leader to all participants
(a, b, and c mean you can: Transfer global case owner to someone else)

Special case

The CERT/CC has reviewed these User Stories and identified one, on publishing advisories, as out of scope. In addition, we have identified as two other User Stories as underspecified.

Not in Scope

User Story **CVD-API-056-56**
I want to publish vulnerability advisories
Roles: Vendor
CVD Phases:
MetaCoord: None

Underspecified

User Story CVD-API-055-124
As a vendor, coordinator or other, I want to be included on a distribution list for advisories which must be clearly identified as public or non-public.
Roles: Vendor. Coordinator, Other
CVD Phases:
MetaCoord: Infrastructure

User Story **CVD-API-054-55**
To what extent is authentication/authorization part of the CVD protocol?
Roles: Finder. Reporter, Deployer, Coordinator, Other
CVD Phases: Discovery, Reporting, Validation and Prioritization, Analysis and Remediation, Public Awareness, Deployment
MetaCoord: Infrastructure

References/Bibliography

1. Allen D. Householder, Garret Wasserman, Art Manion, and Chris King. The CERT Guide to Coordinated Vulnerability Disclosure. https://vuls.cert.org/confluence/ display/CVD. Accessed: 2022-03-01.

2. Allen D Householder, Garret Wassermann, Art Manion, and Chris King. The CERT Guide to Coordinated Vulnerability Disclosure. Technical report, Carnegie-Mellon Univ Pittsburgh Pa Pittsburgh United States, 2017.

3. ISO. Information technology — security techniques — vulnerability disclosure. Standard 29147:2018, International Organization for Standardization, Geneva, CH, October 2018.

4. ISO. Information technology — security techniques — vulnerability handling processes. Standard 30111:2019, International Organization for Standardization, Geneva, CH, October 2019.

Appendix A: Test Case ID Index

This appendix contains a listing of all the test case identifiers by page number.

Revision History

Rev	Description of Change
1	Initial Release

CMU/SEI-2022-TR-CVD-API-PR—DRAFT
DOI: 10.1184/R1/XXXXXXX (Your TC editor will request a DOI number from Research Services: https://servicedesk.sei.cmu.edu/jira/servicedesk/customer/portal/6/create/177.)
Program Name

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM22-0461

http://www.sei.cmu.edu

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.