Reviewing Vulnerability Exploitability eXchange (VEX) Practices

Publication date: March 2025

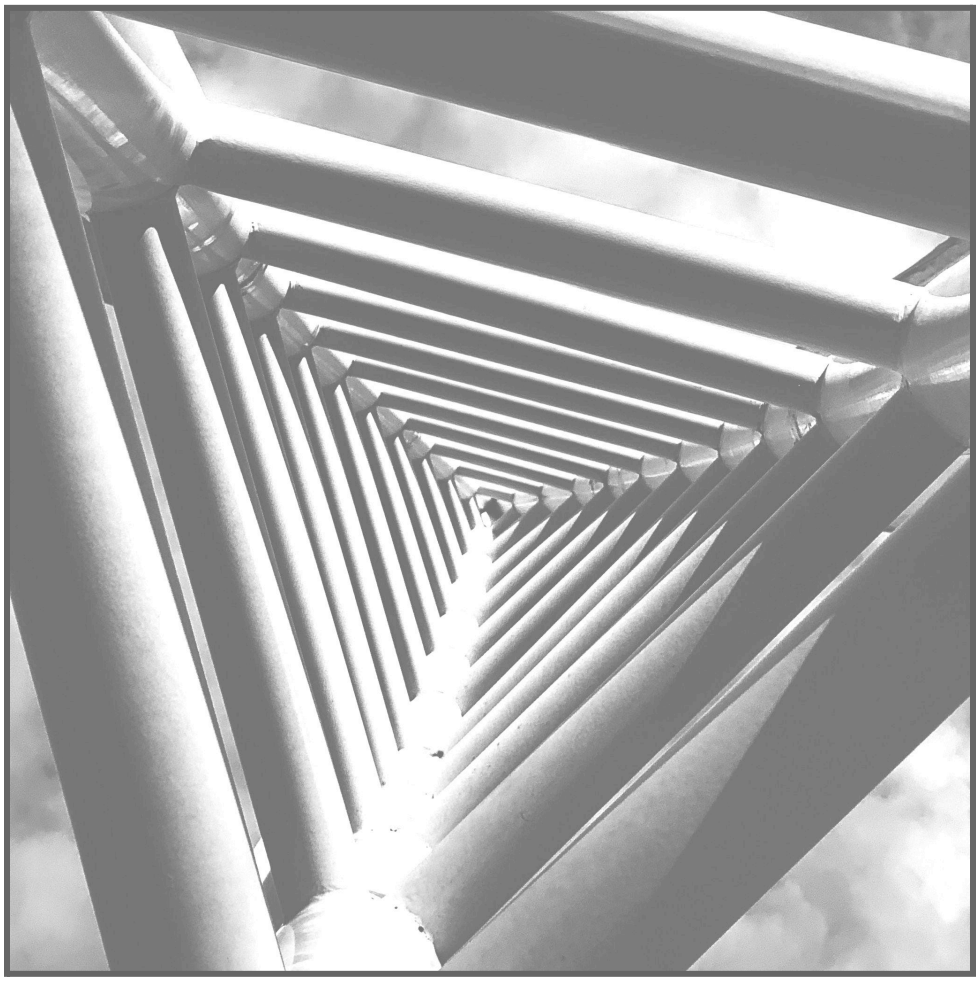

Photo by Cokile Ceoi on Unsplash

Table of Contents

Editor's Note

This paper and the accompanying data were produced by the VEX Working Group as part of the CISA SBOM Community. Pending approval, we expect that the paper and data will be published in the CISA SBOM Resources Library under the terms of the CISA SBOM Community Legal Explanation.[1,2] This may entail additional editorial changes for accessibility purposes.[3]

Overview

Vulnerability Exploitability eXchange (VEX) conveys the extent to which a software-based product or component is affected by a vulnerability. This vulnerability status or, in VEX terms, exploitability, is often related to the use of an upstream dependency that is affected by the vulnerability. While the capability to convey vulnerability status is not new, VEX offers a standardized way to convey status that incorporates supply chain relationships and Software Bills of Materials (SBOM).[4]

The concept of VEX was introduced in 2021 during the National Telecommunications and Information Administration (NTIA) Multistakeholder Process for Software Component Transparency.[5] To better understand how VEX is being used or considered for use today, the VEX Working Group solicited and reviewed current VEX practices with the intention to:

- Collect more information about ongoing assessment and development.
- Confirm or disprove prior beliefs and assumptions.
- Sort out what "end-to-end" VEX looks like.
- Discover roadblocks or gaps in using VEX effectively.
- Determine what activities could overcome the identified gaps.

This review indicates that VEX is being evaluated, tested, and implemented by a variety of early adopters. Out of twenty-seven total respondents in this review, nearly all were either using or considering VEX as part of their vulnerability management activities.[6] Respondents use VEX in different ways. Some use VEX internally and others publish VEX information to external users and customers. Respondents were generally interested in having more VEX information available (particularly from their specific suppliers) and integration with vulnerability advisories, public databases, and vulnerability scanning and management systems. VEX practices contend with typical early-stage issues. Multiple formats and implementations exist and additional tool support is needed. "End-to-end" VEX will require further experimentation but will likely follow the SBOM model of suppliers at all levels providing authoritative VEX information to downstream users.

---

[1] CISA. SBOM Resources Library | CISA. March 2025.
[2] This document was drafted by the VEX Working Group, a community-driven workstream. For more information, see About this document.
[3] GSA. Section508.gov. March 2025.
[4] CISA. Software Bill of Materials (SBOM). October 2024.
[5] NTIA. Vulnerability-Exploitability eXchange (VEX) – An Overview. September 2021.
[6] Subject to intentional selection bias, participants were chosen because of their use of or interest in VEX.

Readers of this document should be familiar with VEX and, more generally, with vulnerability disclosure, response, and management. For background information on VEX, including definitions of VEX data elements and other terminology used in this document, see Minimum Requirements for Vulnerability Exploitability eXchange (VEX),[7] Vulnerability Exploitability eXchange (VEX)–Status Justifications,[8] and Vulnerability Exploitability eXchange (VEX)–Use Cases.[9]

[7] CISA VEX Community Working Group. Minimum Requirements for Vulnerability Exploitability eXchange (VEX). April 2023.
[8] CISA VEX Community Working Group. Vulnerability Exploitability eXchange (VEX)–Status Justifications. June 2022.
[9] CISA VEX Community Working Group. Vulnerability Exploitability eXchange (VEX)–Use Cases. April 2022.

Methodology

In roughly chronological order, the Working Group designed a set of review questions and then solicited responses over a period of several months. As responses came in, the Working Group interpreted, categorized, discussed, and analyzed the results. In the last phase, the Working Group drafted this report.

Text reproduced directly from the review template, including categorized responses, is presented in italics. Text from respondents is properly quoted.

Review Template Design

The review template (see Annex 1) focused primarily on information about respondents' current use of VEX. The template also solicited some minimal demographic information and background on how respondents process and provide vulnerability information independently of VEX.

Response Solicitation

Respondents answered questions using either a Google Form or a document containing a table of questions (see Annex 1). Respondents typically answered questions on their own and some respondents presented and discussed their responses during a VEX Working Group meeting. Partially anonymized response data is available in Annex 2.

The Working Group recognized shortcomings with the review questions, template design, and response solicitation. Some questions were overly open to interpretation or should have been consistently organized into multiple questions. Respondents who filled out the document were able to enter free-form answers for any question and could see the entirety of the questionnaire, while respondents who used the Google Form were conditionally prompted to answer some questions but not others. Affirmative answers to some questions, such as, *Have you started using VEX in any way?* would prompt respondents with further questions about their experience using VEX. Responding *No* to the question *Do you produce VEX?* would skip additional questions regarding VEX production. The form logic is explained in Annex 1.

Response Interpretation

The Working Group categorized and counted responses that were not free-form text. These counts must not be interpreted as anything other than categories and counts of the responses received. Specifically, the responses do not represent interest in or adoption of VEX in the overall population of software suppliers and other VEX users. Similarly, the responses do not indicate population-wide preferences for particular VEX formats or tools. Respondents were overwhelmingly already familiar with, and in many cases, using VEX. This represents a significant and intentional selection bias, as respondents were selected because they were using or considering using VEX.

In rare cases, the Working Group interpreted or modified responses that conflicted with other answers or publicly available information and, when possible, confirmed the changes with the respondent. The Working Group derived some categorical answers from free-form responses. For example *Do you publish or otherwise provide vulnerability information? If so, what formats and automation do you use?* produced nine distinct categories for *Vulnerability Information Format* (see Table 7).

Tables in the Responses section show counts of categorical responses. Some tables may contain fewer or more than twenty-seven responses. Reasons for this include:

- Multiple categorical answers were identified and extracted from a single response.
- Some questions were not provided to all respondents due toform logic (see Annex 1).
- Blank responses were filled in or responses were interpreted and adjusted when the Working Group was highly confident about the change (for example, using authoritative public references or confirming with the respondent).

The response data can be found in Annex 2.

Analysis

The Working Group studied and discussed the responses and categorized counts, developed user stories, and captured significant insights.

Responses

This section describes the responses in rough order of the review template (see Annex 1). Each question is presented in a text box, followed by an explanation of the question and trends in responses. Unusual or otherwise outstanding answers are highlighted. As noted above, some tables may contain more or less than twenty-seven responses.

Demographics

Please provide the organization type, industry, sector.

Respondents first answered this question in free-form text. To categorize the responses, each response was assigned one or more corresponding critical infrastructure sectors.[10] Not all respondents were based in the United States and thus were not all covered specifically under the CISA Critical Infrastructure Sectors list. Still, all responses mapped well to either *Information Technology, Communications, Manufacturing*, or *Healthcare and Public Health*, as shown in Table 1.

Some respondents fit in multiple sectors. Eighteen respondents were assigned only to *Information Technology*, three were assigned to *Information Technology* and *Communications*, one was assigned to *Information Technology* and *Manufacturing*, one was assigned to *Healthcare and Public Health*, and four were assigned to *Manufacturing* only.

Table 1: Sector Demographics

Sector	Total Responses	Exclusive Responses
Information Technology	22	18
Communications	3	0
Manufacturing	5	4
Healthcare and Public Health	1	1

[10] Adapted from CISA Critical Infrastructure Sectors. September 2024.

Please provide the organization size in rough terms of full-time equivalent (FTE) staff.

Respondents answered with an estimate of the number of full-time equivalent staff that they employ. Responses were divided into bins on a logarithmic scale to capture the significant range of organizations' sizes. Five respondents employ over 100,000 people. Nine respondents employ between 10,000 and 100,000 people. Two respondents employ between 100 and 10,000 people, and eleven employ fewer than 100 people. Two respondents have only one employee. This information is reflected in Table 2.

Table 2: Full-Time Employee Count

Full-time equivalent	Responses
< 10	5
10 < 100	6
100 < 1,000	1
1,000 < 10,000	1
10,000 < 100,000	9
> 100,000	5

Phases

Which of these phases best describes your use of VEX? Select all that apply.	☐ Production ☐ Testing ☐ Evaluating ☐ None ☐ Other (please explain)

Respondents were allowed to select multiple phases. Nineteen of twenty-seven respondents said they were in the *Production* phase, fourteen said they were *Testing*, and fifteen said they were *Evaluating*. Two respondents only selected *Testing*, and four respondents only selected *Evaluating*. The total, cumulative count of respondents who selected each phase as well as the count of respondents who selected exclusively one phase are shown in Table 3 below.

Table 3: VEX Phases

VEX Phase	Total Responses	Exclusive Responses
Evaluating	15	4
Testing	14	2
Production	19	8

Responses of Interest

Three respondents included additional comments or marked *Other*. One stated that they were performing "internal pilot testing" for specific vulnerabilities and products, which the Working Group categorized as *Testing*. Another respondent reported that they were "enabling internal automation activities," which was disregarded.

The third respondent who marked *Other* made an interesting distinction between two "dimensions" of VEX. In their own words, "The first dimension is the internal application of VEX to capture the exploitability assessment data. The second dimension is the creation of a VEX artifact and dissemination of this VEX artifact." This respondent said that they would be in the Production phase of "internal application of VEX to capture exploitability," and in the Evaluating phase of "creating and disseminating VEX artifacts." This respondent "envisions an ecosystem of security scan tools and other third party tooling having a (near) real-time ability to ingest and process vendor-provided information on known vulnerability exploitability. This flow is based on standardized formats such as the Common Security Advisory Framework (CSAF) and industry-standard distribution mechanisms."[11] This distinction is not reflected in the chart below, as the respondent also selected *Production*, *Testing*, and *Evaluating*. This response of *Other* was disregarded in Table 3.

Roles

Which of these *roles* best describes your use of VEX? Select all that apply.	☐ Producer ☐ Consumer ☐ Developer of VEX specifications, formats, standards ☐ Developer of VEX tools, services, or applications for use by others ☐ None ☐ Other (please explain)

Respondents were allowed to select multiple roles. The most common response was the *Producer* role, which twenty-two respondents selected. Eight respondents selected *Consumer*, all eight of which also selected *Producer*. Nine respondents selected *Developer of VEX tools,*

[11] OASIS. Common Security Advisory Framework (CSAF). October 2024.

services, or applications for use by others. Three respondents selected *Developer of VEX specifications, formats, or standards*. Two respondents selected *Other*, as they represent a group or consortium that is evaluating VEX. One respondent did not answer but is publicly producing VEX information so their response was counted as *Producer*.

The total count of respondents who selected each role as well as the count of respondents who exclusively selected one role are displayed in Table 4.

Table 4: VEX Roles

VEX Role	Total Responses	Exclusive Responses
Producer	22	11
Developer of VEX tools, services, or applications for use by others	9	3
Developer of VEX specifications, formats, standards	3	1
Consumer	8	0
Other	2	1

First Use of VEX

When did you start using VEX?

The Working Group interpreted this to be the earliest date at which the respondent started using VEX in any capacity or role. The earliest adoption year reported was 2020. Three respondents started using VEX in 2021, four started in 2022, fifteen started in 2023, and two more started in 2024. Two respondents have not yet begun using VEX. These counts are reflected in Table 5.

Table 5: First Use of VEX

Year	Responses
2020	1
2021	3
2022	4
2023	15
2024	2
Not Using VEX	2

Vulnerability Information

Do you publish or otherwise provide vulnerability information? If so, what formats and automation do you use?

Respondents answered *Yes* or *No* and explained their formats and automation in open-ended text. Twenty-two of the twenty-seven respondents provide vulnerability information in some form. Several respondents provided vulnerability information in multiple formats. *CSAF* was the most common format used to share vulnerability information, with twelve respondents. Other respondents reported using the *Minimum VEX Requirements*,[12] *OpenVEX*,[13] *CycloneDX*,[14] *CVRF*,[15] *OVAL*,[16] *OSV*,[17] Security Advisories with manually-entered information, and custom, proprietary formats. Most respondents' vulnerability publication processes were already automated to some extent, and most respondents provide vulnerability advisories publicly, privately to customers, or both.

The count of respondents who do and do not provide vulnerability information is displayed in Table 6. The frequency of reported use of different vulnerability information formats is displayed in Table 7. As noted previously, the sample is heavily biased in favor of respondents who were known or likely to provide vulnerability information.

[12] CISA VEX Community Working Group. Minimum Requirements for Vulnerability Exploitability eXchange (VEX). April 2023.
[13] OpenSSF. OpenVEX. October 2024.
[14] OWASP. CycloneDX. October 2024.
[15] OASIS. CSAF Common Vulnerability Reporting Framework (CVRF) Version 1.2. October 2024.
[16] OVAL. The OVAL Community Guidelines. October 2024.
[17] OpenSSF. OSV Schema. October 2024.

Table 6: Publishing Vulnerability Information

Do you Publish or Provide Vulnerability Information to Users?	Responses
Yes	22
No	5

Table 7: Vulnerability Information Format

Vulnerability Information Format	Responses
CSAF	12
CycloneDX	4
Security advisory	4
OpenVEX	3
CVRF	2
Minimum VEX Requirements	1
OVAL	1
OSV	1
Proprietary	1
Do Not Publish	5

VEX Production

Do you produce VEX? How?

Respondents answered *Yes* or *No* and explained in open-ended text how they produce VEX. Twenty-two out of the twenty-seven respondents produce VEX in some capacity. See Table 8.

The most common format used to produce VEX is *CSAF*, which is used by eight respondents. Six respondents use *OpenVEX* and five use *CycloneDX.* Three respondents produce VEX in multiple formats. Five respondents do not produce VEX at all. See Table 9.

Most of the organizations that do produce VEX use customized, internal tools or processes. Fifteen respondents report using their own internal tools to produce VEX. A few respondents use *Secvisogram*[18] or *OpenVEX*. See Table 10.

Table 8: VEX Production

Do You Produce VEX?	Responses
Yes	22
No	5

Table 9: VEX Production Format

VEX Production Format	Responses
CSAF	12
OpenVEX	6
CycloneDX	5
Minimum VEX Requirements	1
SPDX	1
Do Not Produce VEX	5

[18] BSI. Secvisogram. October 2024.

Table 10: VEX Production Tools

VEX Production Tools	Responses
Internal	15
OpenVEX	2
Secvisogram	2
SPDX Tools	1
Interlynk Platform	1
Cisco Vulnerability Repository	1
Manual Documentation	1
Do Not Produce VEX	5

Vulnerability Selection

For which vulnerabilities do you produce VEX? How do you select the vulnerabilities for which VEX is produced?

For those respondents who do produce VEX, it is common to produce VEX only for vulnerabilities that can affect the organization's own products. Some respondents employ automated processes for checking which vulnerabilities may affect relevant products or components. These respondents often use SBOM for mapping vulnerabilities to products or have vulnerability scanning capabilities built into their development processes. Some respondents use both. A few respondents additionally produce VEX for high-profile vulnerabilities even if they do not affect the respondents' products.

Some respondents were not yet producing VEX at all, or in a limited capacity. Respondents with limited VEX production generally prioritize new or high-profile vulnerabilities or vulnerabilities that were already confirmed to affect relevant products. Some respondents used severity and exploitability metrics such as CVSS,[19] EPSS,[20] and the CISA KEV[21] to help select vulnerabilities for VEX production.

[19] FIRST. Common Vulnerability Scoring System SIG. November 2024.
[20] FIRST. Exploit Prediction Scoring System (EPSS). November 2024.
[21] CISA. Known Exploited Vulnerabilities Catalog. November 2024.

Supporting Evidence

To what extent do consumers of your VEX information seek or ask for evidence supporting VEX status and justification?

In general, the responses indicate that VEX consumers were not asking for much additional evidence or justification beyond what is provided by existing vulnerability information and security advisories. However, many respondents who share VEX expect this to change as VEX proliferates. Seven respondents specified that nobody had asked them for additional evidence at all. Respondents with experience sharing VEX reported that consumers generally trust their status justifications and attestations.

Responses of Interest

One respondent raised the issue of multiple VEX sources: “How do I trust this statement, and what do I do if I have conflicting statements from multiple suppliers?” This response highlights an important issue that is discussed further in Deconflicting VEX Information.

Another respondent reported that requests for VEX evidence had been “very very quiet” and that “not a lot of customers have asked for evidence, but we know that's definitely going to change in the future.”

Another respondent noted the distinction between the questions “Are you sure of/do you trust status?” and “How severe is the vulnerability?” but only reported being asked about confidence in the severity assessment.

One respondent reported that “there are more and more customers asking ‘how can we receive vulnerability information.’”

What evidence do you provide to support VEX status and justification?

Most respondents reported that users were not asking for additional evidence to support VEX statuses, but some respondents provide evidence or at least additional context. Several VEX producers stated that they provide digitally-signed VEX documents or human-written justifications to give VEX consumers more detail and context about affected products.[22] At least one respondent used VEX and CSAF data elements to provide supporting evidence.

Other respondents provided the following as evidence or justification for VEX status:

- “references”
- “significant vulnerability information”
- “developer statements”
- “realtime context about running workloads”
- “free-form text”

[22] Digital signatures provide integrity, authenticity, and non-repudiation but do not guarantee that VEX information is accurate.

- “code_not_present”
- “human-written justification”
- “reports from vulnerability scanners”
- “a very detailed SBOM”
- “notes with the CVE information obtained from upstream databases like NVD and then an impact assessment”
- “manual triage”
- “references as well as CWE information”
- “as much detail as they wish”
- “a description about the status”
- “self-attestation proclamation”
- “documentation of VEX processes”

Responses of Interest

One respondent reported that “we provide the justifications in the VEX status. However, there are no plans to show evidence (i.e., source code access, etc.).” Another respondent reported that “no VEX status and justification information is shared externally and the only ‘evidence-sharing’ happens through trusted channels established in regular business processes (i.e., support).”

What evidence do you use, or lack, to assess trust in VEX status and justification?

Fifteen respondents did not answer. Seven respondents specified that they do not use any evidence or that they simply trust the VEX supplier. A few respondents employ measures for digitally signing VEX documents. Others reported verifying VEX status using context and details about the vulnerability or component of interest. One respondent uses a “validator tool” that is “built into our pipelines to check that everything is according to CycloneDX specification.”

Sharing

Do you share VEX? With whom? How?

Fourteen respondents share VEX in some capacity, and thirteen do not. *Do not share* in Table 12 includes all respondents who did not report sharing VEX, either because they do not produce VEX or because they do not share with anyone. Six respondents produce VEX but do not report sharing it. Of the respondents who do share VEX, five make their VEX publicly available, six share VEX only with customers, and three only share VEX internally. These counts are displayed in Table 11 and Table 12.

Table 11: VEX Sharing

Do You Share VEX?	Responses
Yes	14
No	13

Table 12: VEX Sharing Audience

With Whom do You Share VEX?	Responses
Customers only	6
Public	5
Internal	3
Do not share	13

VEX Consumption

Do you consume VEX? From where? How?

Ten respondents consume VEX somehow, and seventeen do not consume VEX at all. Those who do consume VEX receive it from public sources, other software suppliers with their own mature VEX processes, or consume internally-produced VEX. These counts are displayed in Table 13.

One respondent specifically noted consuming internally-produced VEX, but their suppliers do not produce VEX. Some respondents consumed VEX from internal sources or were able to consume VEX from external sources, even if their suppliers do not provide it.

Table 13: VEX Consumption

Do You Consume VEX?	Responses
Yes	10
No	17

Do you want to consume VEX?

Two respondents said *No,* eleven said *Yes*, and fourteen did not answer. These counts are displayed in Table 14. Note that respondents who answered *Yes* to the previous question (*Do you consume VEX?*) via the Google Form were not prompted with this question.

Table 14: Desire to Consume VEX

Do You Want to Consume VEX?	Responses
Yes	11
No	2
Did not Answer	14

If so, how would you like to consume VEX?

Respondents were generally interested in further automation and technical integration of VEX information. There is a general expectation that more suppliers will start producing VEX, which will make consumption easier. Various responses noted that a single, widely-adopted format for VEX would be beneficial.

VEX Development

Do you develop (produce) or maintain VEX tools, systems, or formats?

If so, please summarize.

Almost all respondents (twenty-two) used some kind of specialized process or tools, most of which were internally developed and not publicly available. Many respondents integrated freely available formats and tools including CSAF, CycloneDX, OpenVEX, and SPDX.[23] Four respondents did not develop or maintain any VEX tools, systems, or formats.

Why are you using or evaluating VEX?

Generally, respondents were interested in VEX because it enables automatable, machine-readable sharing of vulnerability information. Several respondents specifically liked that VEX is compatible with vulnerability scanning tools and SBOM. Respondents also saw value in VEX to help inform security decisions and streamline support costs for both suppliers and users. Some respondents were interested in better integration with vulnerability scanning tools to improve accuracy and reduce false-positive detections.

[23] The Linux Foundation. System Package Data Exchange (SPDX). October 2024.

VEX Experience

What works?

Many respondents see VEX as a fundamentally good idea although still in early stages of adoption. One reported specifically that VEX “solves a big pain point in vulnerability management.” Some respondents noted that CSAF and CycloneDX implementations work well. Others noted that the status justifications were particularly useful.

What does not work?

Many respondents struggled with compatibility and interoperability. The number and variety of VEX-related tools, many of which are not cross-compatible, complicates VEX adoption. Some respondents report difficulty associating vulnerabilities with the correct components. This is likely due to the complexity of supply-chain relationships and software identification at a global scale and may not be addressed by VEX directly. Some respondents also noted that VEX is resource and time intensive.

What would you change?

In general, respondents were interested in greater compatibility and interoperability among VEX tools. Respondents commonly suggested better standardization and unified formats across the VEX environment.

What other VEX practices do you suggest we review?

This question was asked primarily to discover other VEX efforts to review. Respondents, however, provided a wide variety of comments including:

- “‘Fixed’ Workflow, including Fixed Action Codes”
- “Concerns that the current guidance does not follow the PSIRT framework”
- “VEX Signing so consumers know the VEX statement is genuine and immutable”
- “Guidance for the creation of ‘Affected’ VEX statements. What information is needed? What communication is needed?”
- “How does a VEX statement relate to a Security Notification?”
- “How to reference a VEX Document”
- “Referencing in CSAF the Included Component that has the vulnerability”
- “Embedded VEX in SPDX”
- “Previously unknown vulnerabilities. Vulnerabilities against services, etc.”
- “Integration of advisory and VEX profiles”
- “The publishing of VEX itself, i.e. when do we really want to make a VEX public available for consumers.”
- “How is non-exploitability being evaluated?”
- “More structure to the evaluation criteria”

- “Integration with SBOMs, Trust Model, VEX Discoverability”

Many of these comments can be associated with known issues, many of which have practical solutions. Other comments represent newly-surfaced issues that likely require additional Discussion.

User Stories

The following VEX user stories are based on the reviews and discussions in the Working Group during the review process. This set of user stories is not necessarily comprehensive and it is not intended to limit the development of additional stories. While there is some natural overlap, these user stories are not intentionally aligned with the use cases described in Vulnerability Exploitability eXchange (VEX)–Use Cases.[24]

Table 15: User Stories

	As a…	**I want to…**	**In order to…**
1	Software system supplier, specifically a product security response capability, such as a PSIRT[25]	Provide vulnerability status information to users in an automated way	Enable more effective and faster vulnerability response
2	"	"	Reduce support requests and corresponding costs to both users and suppliers
3	"	Better integrate with vulnerability scanning and management tools	Return more accurate scanning results, specifically fewer false-positive detections
4	"	"	Reduce support requests and corresponding costs to both users and suppliers
5	Medical device manufacturer	Receive SBOM and vulnerability information, including VEX, from suppliers of upstream components	Discover known vulnerabilities in upstream components
6	"	"	Remediate vulnerabilities prior to launch

[24] CISA VEX Community Working Group. Vulnerability Exploitability eXchange (VEX)–Use Cases. April 2022.
[25] FIRST. PSIRT Services Framework. August 2024.

	As a…	I want to…	In order to…
7	"	"	Better understand risk associated with vulnerabilities in fielded products
8	"	"	Notify users about risk associated with vulnerabilities in fielded products
9	Software system supplier, specifically a development capability incorporating upstream software and hardware components	Collect and analyze SBOM and VEX for upstream components	Reduce risk and maintenance costs by selecting upstream suppliers that provide consistent, timely, and practical vulnerability exploitability information
10	Enterprise SOC, vulnerability or threat management capability	Quickly and easily ingest VEX from suppliers in an automated fashion at scale	Determine exposure to current and emerging vulnerabilities and mitigation advice
11	"	Use existing solutions, tools, and data as much as possible	Minimize cost and complexity of adding new solutions, tools, and data
12	CSIRT[26] with public safety mandate	Collect and analyze VEX for a set of suppliers	Better assess risk to public safety
13	CSIRT with public safety mandate	Track status for known vulnerabilities	Better inform incident response, for example, determining which vulnerabilities may be involved in an incident
14	End user	Collect and analyze VEX from suppliers and correlate vulnerability status with assets	Better assess risk and prioritize vulnerability mitigation activity
15	"	Collect and analyze VEX from suppliers and potential suppliers	Assess vulnerability management practices of suppliers and potential suppliers

[26] FIRST. Computer Security Incident Response Team (CSIRT) Services Framework. August 2024.

	As a…	I want to…	In order to…
16	Vulnerability scanning and management supplier	Collect and analyze VEX from suppliers of software scanned by users	Improve scan result quality, specifically reduce false-positive detections related to assumed inheritance of upstream vulnerabilities
17	Regulator	Collect and analyze SBOM and VEX information	Determine compliance (including enforcement and exceptions) with regulations that apply to a product or sector
18	"	"	Investigate cases and incidents to determine contributing actions, knowledge, and timelines
19	Auditor or assessor	Collect and analyze SBOM and VEX information	Check compliance against internal or external regulations or requirements and require or propose changes

Discussion

Given the early stages of VEX adoption and the biased sample used for the review, the Working Group was hesitant to draw firm conclusions. Nonetheless, the review highlighted several key insights that might help close gaps and enable greater VEX adoption. As stated previously, the original goals of this review were to:

- Collect more information about ongoing assessment and development.
- Confirm or disprove prior beliefs and assumptions.
- Sort out what “end-to-end” VEX looks like.
- Discover roadblocks or gaps to using VEX effectively.
- Determine what activities could overcome these gaps.

These goals were generally met, with the possible exception of clearly defining End-to-End VEX, which is further explained below. VEX users saw potential for improving vulnerability detection and management, but there were still typical early-stage obstacles to widespread adoption. The VEX landscape is fragmented and immature, there were multiple formats and tools with varying compatibility, and there were isolated VEX producers and consumers who were missing VEX in their supply chains. Consumers wanted more of their suppliers to provide VEX and respondents generally wanted vulnerability databases, scanners, and management systems to support VEX. Based on this review, there is significant interest from the growing VEX community in working to overcome these obstacles.

End-to-End VEX

The responses did not indicate the existence of a significant cross-organizational “end-to-end” VEX ecosystem, and discovering and exchanging VEX information at scale has not been materially tested. This is expected due to the limited number of VEX producers and consumers. Even in this early stage of adoption, eleven out of twenty-seven respondents currently provide VEX information as part of their vulnerability disclosure practices. It makes sense that VEX, along with other vulnerability information, would follow the SBOM model of suppliers at all levels providing information to their direct downstream users along supply chains.

Better Vulnerability Detection

Some respondents noted concerns about false-positive detections by vulnerability scanning and management systems.[27] These systems often assume that a vulnerability in an upstream component is inherited with the same exploitability, impact, and severity by the downstream product. In many cases, this assumption is incorrect. The downstream product may not be affected or exploitable by the vulnerability in the upstream component, due to the way the upstream component is used in the downstream product. Mistaken detections increase costs to both users and suppliers to further investigate.

[27] In one sense, “false positive” can indicate that a “true positive” vulnerability detection is not exploitable. In other cases, a “false positive” is just that, a mistaken vulnerability detection.

VEX may be able to improve the quality and efficiency of information exchanged among the triad of software suppliers, users, and vulnerability scanners. For example, if a scanner detects a component based on a known-vulnerable version string, a corresponding VEX statement could explain that the vulnerability is not exploitable because the vulnerable code is not present or not accessible. A VEX statement could also be used to decrease the impact or severity assessment of the upstream vulnerability to the downstream product. VEX could be used to improve the results of vulnerability scanning and management systems through an additional external process or by incorporation into the systems themselves.[28]

Deconflicting VEX Information

An important point was raised in a response to the Supporting Evidence questions. Those questions explore what evidence consumers seek to help determine trust in VEX information. While any assessment may be subject to error or influence, different VEX producers will likely have different information available leading to potentially different VEX status assertions. In a future with multiple sources of VEX information, it will be necessary to collect, associate, and resolve conflicts from multiple sources. For example, an upstream component supplier, a supplier incorporating that component into a product, a software composition analysis tool, and a vulnerability scanner may all generate subtly or materially different VEX information about the same vulnerability and components. The accuracy of this collection of VEX information may be relative to the consumer's knowledge and position in the supply chain, which is to say, there may be multiple truths. Consumers will also make their own subjective determinations about the extent to which they trust different sources of VEX information, even in the absence of conflicting information.

Vulnerability Database Integration

Suppliers often integrate their vulnerability information with widely-used vulnerability databases such as CVE.[29] Assuming more suppliers begin providing VEX information, vulnerability databases may want to support VEX. The review template asked respondents if they provided vulnerability information and if so, in what format. While these questions do not directly assess integration with vulnerability databases, such databases often collect public information with or without the direct participation of the sources. The CVE Program operates arguably the most well-known global and public vulnerability database, and many other databases incorporate CVE data or reference CVE IDs. Vulnerability databases today, including CVE, do not natively support VEX. In particular, the databases lack mechanisms to explicitly reference a vulnerable upstream component or subcomponent. The CVE Program is discussing how to express the vulnerability status of a downstream product with respect to a vulnerability in an upstream component.[30] While the outcome of these discussions is not clear, it seems likely that VEX or

[28] Trivy, for example, has experimental support for VEX. Trivy (v0.55). Vulnerability Exploitability eXchange. August 2024.
[29] CVE Program. CVE Program. October 2024. Other similar databases exist such as OSV and GSD.
[30] CVE Program. GitHub issues with 'VEX'. October 2024.

VEX-like functionality will be a near-term consideration for at least CVE and possibly other vulnerability databases.

More VEX

This review revealed a significant lack of VEX sources. This is not unexpected, given the early stage of adoption.

Most respondents were interested in both analyzing incoming VEX information and using VEX to share vulnerability information internally and externally to their organization. To do so requires more sources of VEX information. Sources may include first-party suppliers and third-party software composition analysis capabilities. Multiple respondents noted that while they have the capability to consume VEX information, their suppliers do not provide it. In a separate study conducted by Blackberry, 42% of respondents ask for VEX from their suppliers, and an additional 40% plan to ask in the future.[31] As suppliers and maintainers begin to share VEX statements more broadly, most expect to realize improvements in their own vulnerability management efforts.

[31] Coleman Parkes, BlackBerry. Software supply chain research. May 2024.

Contributors

This document was written by the CISA SBOM VEX Working Group. Contributors included:

Allan Friedman, CISA
Art Manion
Bruce Lowenthal, Oracle
Charlie Hart
Chris Gregoire, Boston Scientific
Christopher "CRob" Robinson, Intel, OpenSSF
Craig Trump, HPE
Deanna Medina, United Airlines
Duncan Sparrell, sFractal Consulting
Ed Heierman, Ph.D., Abbott
Christine O'Leary, Intel
Eoin Wilson-Manion
François Ambrosini, Huawei
Jeremiah Stoddard, INL
John Cavanaugh, Internet Infrastructure Services Corporation
Mike O'Connor, HPE
Przemysław Roguski, Red Hat
Ricardo Reyes, Tidelift
Saquib Saifee, IBM
Syed Zaeem "Z" Hosain, Aeris Communications Inc.
Thomas Schmidt, BSI
Victoria Ontiveros, CISA

Annex 1: Review Template

This template was used to conduct reviews of VEX practices.

Question	Response
Reviewer	Name
Method	How was the review conducted, e.g., in VEX WG, reviewer and respondent met directly, independently
Date	yyyy-mm-dd
Respondent	Full name Title (optional) Organization, sub-organization (VEX-relevant part of organization)
Organization type, industry, sector	CISA Critical Infrastructure Sectors[32]
Organization size	Approximate number of full-time equivalent employees
Summary	May be easier to write this after collecting other information
References	Relevant URLs (which may also appear throughout response)
Which of these *phases* best describes your use of VEX? Select all that apply.	☐ Production ☐ Testing ☐ Evaluating ☐ None ☐ Other (please explain)

[32] Adapted from CISA Critical Infrastructure Sectors. September 2024.

Which of these *roles* best describes your use of VEX? Select all that apply.	☐ Producer ☐ Consumer ☐ Developer of VEX specifications, formats, standards ☐ Developer of VEX tools, services, or applications for use by others ☐ None ☐ Other (please explain)
When did you start using VEX?	
Do you publish or otherwise provide vulnerability information to users? If so, what formats and automation do you use?	Including non-VEX vulnerability information
Do you produce VEX? How?	Include tools and formats
For which vulnerabilities do you produce VEX? How do you select the vulnerabilities for which VEX is produced?	
To what extent do consumers of your VEX information seek or ask for evidence supporting VEX status and justification?	
What evidence do you provide to support VEX status and justification?	Includes documentation of VEX processes
Do you share VEX? With whom? How?	Include tools and formats
Do you consume VEX? From where? How?	Include tools and formats
Do you want to consume VEX?	

If so, how would you like to consume VEX?	
What evidence do you use, or lack, to assess trust in VEX status and justification?	Includes documentation of VEX processes
Do you develop or maintain VEX tools, systems, or formats? If so, please summarize.	
Why are you using or evaluating VEX?	
What works?	
What does not work?	
What would you change?	
Are you interested in discussing VEX implementation with other VEX implementers? If so, and you are willing to, please provide an email address.	
What other VEX practices do you suggest we review?	

The template was also converted into a Google Form. Most respondents used the form, which included conditional logic that resulted in some questions being asked and others being skipped.

“Do you produce VEX?”
“Yes” asks:

- “How do you produce VEX (include tools and formats)?”
- “For which vulnerabilities do you produce VEX?”
- “How do you select the vulnerabilities for which VEX is produced?”

- “To what extent do consumers of your VEX information seek or ask for evidence supporting VEX status and justification?” “What evidence do you provide to support VEX status and justification?”

“Do you share VEX?”
“Yes” asks:
- “With whom do you share VEX?”
- “How do you share VEX?”

“Do you consume VEX?”
“No” asks:
- “Do you want to consume VEX?”
- “Yes” asks question:
    - How would you like to consume VEX?

“Yes” asks:
- “From where do you consume VEX?”
- “How do you consume VEX?”
- “What evidence do you use, or lack, to assess trust in VEX status or justification?”

“Are you evaluating VEX for current or future use?”
“No” skips:
- “Why are you using or evaluating VEX?”
- “What works?”
- “What does not work?”
- “What would you change?”
- “Summary & Relevant references” section

Annex 2: Response Data

Response data is available in the CISA SBOM Community Document Repository.[33] Respondents chose from three options about how their data should be published and anonymized:

1. Remove all identifying information, including organization and individual names, product and project names, and URLs. This was the default option.
2. Identify organizations, products, and projects, but remove identifying information about individuals.
3. Delete all data from the published set. Response data was used for analysis, but not published.

The response data contains both raw data (anonymized according to the respondents' preferences, but not otherwise edited) and adjusted data (typically categorized or normalized as described in Responses). Identifying information, organizations' names, and product names have been anonymized as 'Respondent' or 'Product' in some of the data. Column names for adjusted data use the prefix 'adjusted_'.

[33] CISA SBOM Community Document Repository. Reviewing VEX Practices. March 2025.