1.0 Supplier Related Vulnerability (SRV)

1.1 General Description

Supplier Related Vulnerability measures the percentage of vulnerabilities found that are caused by a supplier.

1.2 Purpose

This measurement is an assessment of the organization's supply chain security processes.

1.3 Applicable Business Categories

This measurement applies to all business categories.

1.4 Detailed Description

a) Terminology
- Critical Vulnerability – NIST NVD CVSS v3.0 score of 9 or greater
- High Vulnerability – NIST NVD CVSS v3.0 score of equal to or greater than 7 but less than 9
- Medium Vulnerability – NIST NVD CVSS v3.0 score of equal to or greater then 4 but less than 7
- Low Vulnerability – NIST NVD CVSS v3.0 score of less than 4

b) Counting Rules

1) Vulnerabilities shall be reported in the month that they have been discovered or reported to the organization by an outside party and only in that month.

2) SRV shall be reported in the criticality classification at the time the data is calculated for reporting.

3) If the source of the vulnerability cannot be determined, it shall be counted as supplier caused.

c) Counting Rule Exclusions

1) If the issue is determined to not be a vulnerability , it shall be excluded from the data reporting.

d) Calculations and Formulas

1) The SVR measurements are calculated monthly as shown in table 1-2.

Table 1-1 SRV Notation

Identifier	Business Categories	Definition
SRVs1	All	Number of Critical supplier related vulnerabilities found or reported in the report period
SRVt1	All	Total number of Critical vulnerabilities found or reported in the period
SRVs2	All	Number of High supplier related vulnerabilities found or reported in the report period
SRVt2	All	Total number of High vulnerabilities found or reported in the period
SRVs3	All	Number of Medium or Low supplier related vulnerabilities found or reported in the report period
SRVt3	All	Total number of Medium or Low vulnerabilities found or reported in the period

Table 1-2 SRV Measurement Identifiers and Formulas

Identifier	Title	Formula	Note
SRV1	Critical Supplier Related Vulnerability	100 x (SRVs1 / SRVt1)	% completed on time
SRV2	High Supplier Related Vulnerability	100 x (SRVs2 / SRVt2)	% completed on time
SRV3	Medium or Low Supplier Related Vulnerability	100 x (SRVs3 / SRVt3)	% completed on time

e) Reported Data and Format

1) Monthly data shall be reported per the frequency and method noted in the SCS 9001 Data Reporting System documentation.

2) The SRV measurements shall be reported for each month and each business category with data elements as shown in Table 1-3.

Table 1-3 SRV Data Table

Identifier	Value
MeasurementID	SRV
SRVs1	Number of Critical supplier related vulnerabilities found or reported in the report period
SRVt1	Total number of Critical vulnerabilities found or reported in the period
SRVs2	Number of High supplier related vulnerabilities found or reported in the report period
SRVt2	Total number of High vulnerabilities found or reported in the period
SRVs3	Number of Medium or Low supplier related vulnerabilities found or reported in the report period
SRVt3	Total number of Medium or Low vulnerabilities found or reported in the period

1.5 Sources of Data

Data for the SRV measurements are derived from

1) the organization’s vulnerability discovery and notification records
2) the organization’s vulnerability root cause analysis records

1.6 Example Calculations

TBD