



Risk-Informed Approach for Verification and Validation

Seemita Pal, Ph.D.

Team Leader, Systems Engineering Team,
Pacific Northwest National Laboratory

May 2022 Technical Talk with ReliabilityFirst

16th May 2022



PNNL is operated by Battelle for the U.S. Department of Energy



Let's Start with a Question!

- What percentage of reported CISA security incidents result from exploits against defects in the design or code of software?
 - 10%
 - 30%
 - 60%
 - 90%

¹https://us-cert.cisa.gov/sites/default/files/publications/infosheet_SoftwareAssurance.pdf

One More Question

- When purchasing an energy delivery system device what questions do you ask the vendor/manufacturer?



Challenges and Opportunities



Alerts and Tips Resources Industrial Control Systems

Industrial Control Systems > ICS-CERT Alerts > Cyber-Attack Against Ukrainian Crit

ICS Alert (IR-ALERT-H-16-056-01)

Cyber-Attack Against Ukrainian Critical Infrastructure

Original release date: February 25, 2016 | Last revised: July 20, 2021

Print Tweet Send Share

Legal Notice

All information products included in <https://us-cert.cisa.gov/ics> are provided "as is" for informational purposes regarding any information contained within. DHS does not endorse any commercial product or service, refer to the appropriate agency for more information. Light Protocol (TLP) marking in the header. For more information about TLP, see <https://us-cert.cisa.gov/tlp>.

Updated July 20, 2021: The U.S. Government attributes this activity to Russian nation-state cyber campaign against Ukrainian critical infrastructure. For more information on Russian cyber activity, see [this report](#).

SUMMARY

On December 23, 2015, Ukrainian power companies experienced unscheduled power outages. There have also been reports of malware found in Ukrainian companies in a variety of critical infrastructure sectors. It is important to note that

U.S. GOVERNMENT ACCOUNTABILITY OFFICE: A Century of Non-Partisan Fact-Based Work

FOR CONGRESS PRESS CENTER CAREERS



REPORTS & TESTIMONIES VIEW TOPICS VIEW AGENCIES BID PROTESTS & APPROPRIATIONS LAW ABOUT

Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness (infographic)

Posted on May 18, 2021

Share this Story:



The recent cybersecurity attack on the Colonial Pipeline Company has led to temporary disruption in the delivery of gasoline and other petroleum products across much of the southeast United States.

In today's WatchBlog post, we look at this attack and the federal government and private-sector response. We here at GAO have been warning of [cybersecurity threats](#) to critical infrastructure for many years, and the need to strengthen the federal role in protecting critical infrastructure, which we reiterated in a report issued in [March](#).

U.S. GOVERNMENT ACCOUNTABILITY OFFICE: A Century of Non-Partisan Fact-Based Work

FOR CONGRESS PRESS CENTER CAREERS



REPORTS & TESTIMONIES VIEW TOPICS VIEW AGENCIES BID PROTESTS & APPROPRIATIONS LAW ABOUT

SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)

Posted on April 22, 2021

Share this Story:



The cybersecurity breach of SolarWinds' software is one of the most widespread and sophisticated hacking campaigns ever conducted against the federal government and private sector. In today's WatchBlog post, we look at this breach and the ongoing federal government and private-sector response. This information is based on publicly disclosed information from federal and private industry sources. We here at GAO are currently conducting a comprehensive review of the breach with plans to issue a public report later this year.



BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

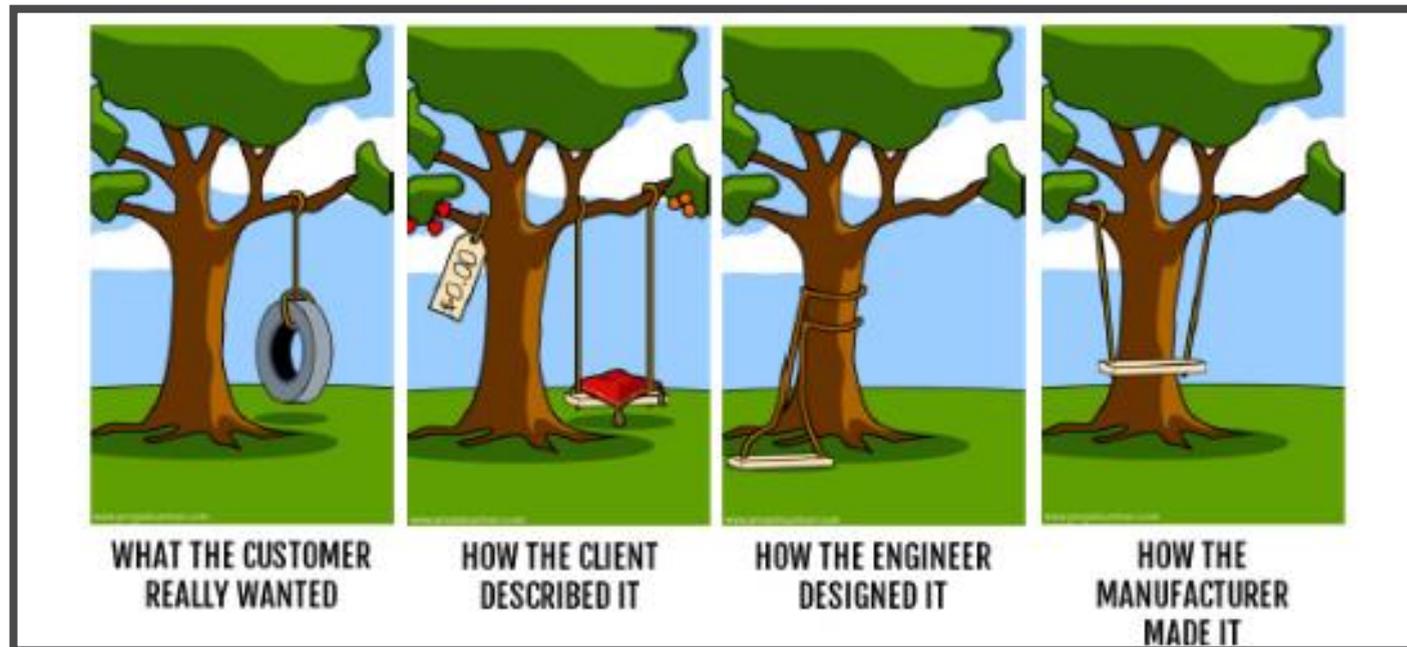
MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the

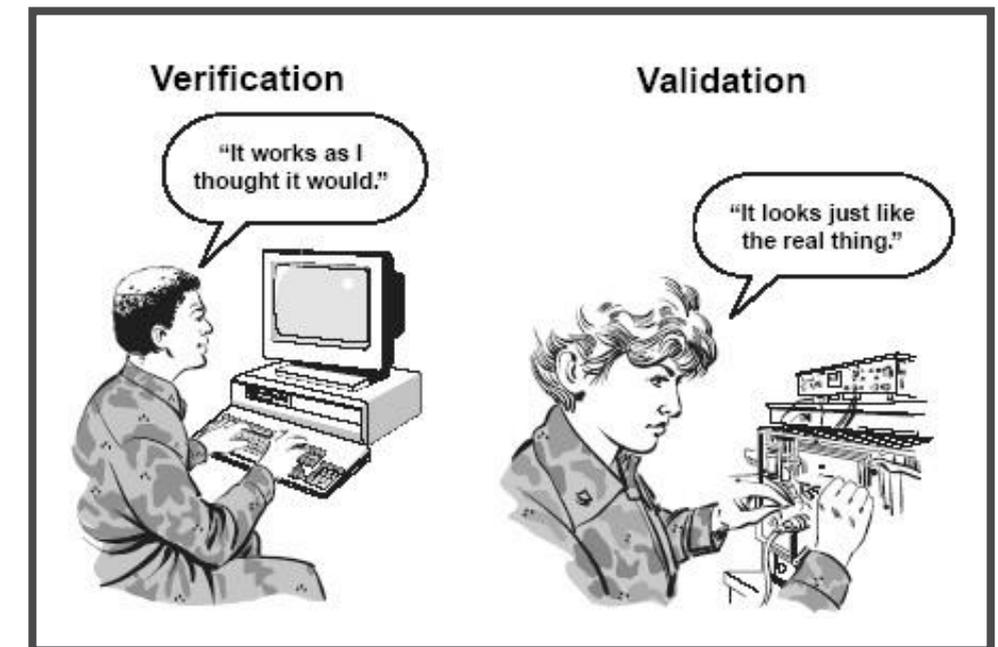
Verification and Validation (V&V)

- **Verification** – have you built something correctly (*does it meet spec?*)
- **Validation** – have you built the right thing (*does it meet user needs?*)



Avoid

Image Source: https://miro.medium.com/max/996/1*nhVE3RkKyhk2kEh3nuk3Lw.png,
Last accessed: 03/13/22



Achieve

Image Source: https://commons.wikimedia.org/wiki/File:Verification_Validation_Accreditation.jpg, Last accessed: 03/13/2022

Challenge 1: Verification and Validation (V&V) Throughout the Lifecycle



Different lifecycle phases, and different stakeholders

Challenge 2: Different Devices Mean Different Risks



Image Source: <https://image.shutterstock.com/image-photo/indoor-medium-voltage-metal-enclosed-260nw-1288606204.jpg> Last Accessed: 03/13/2022

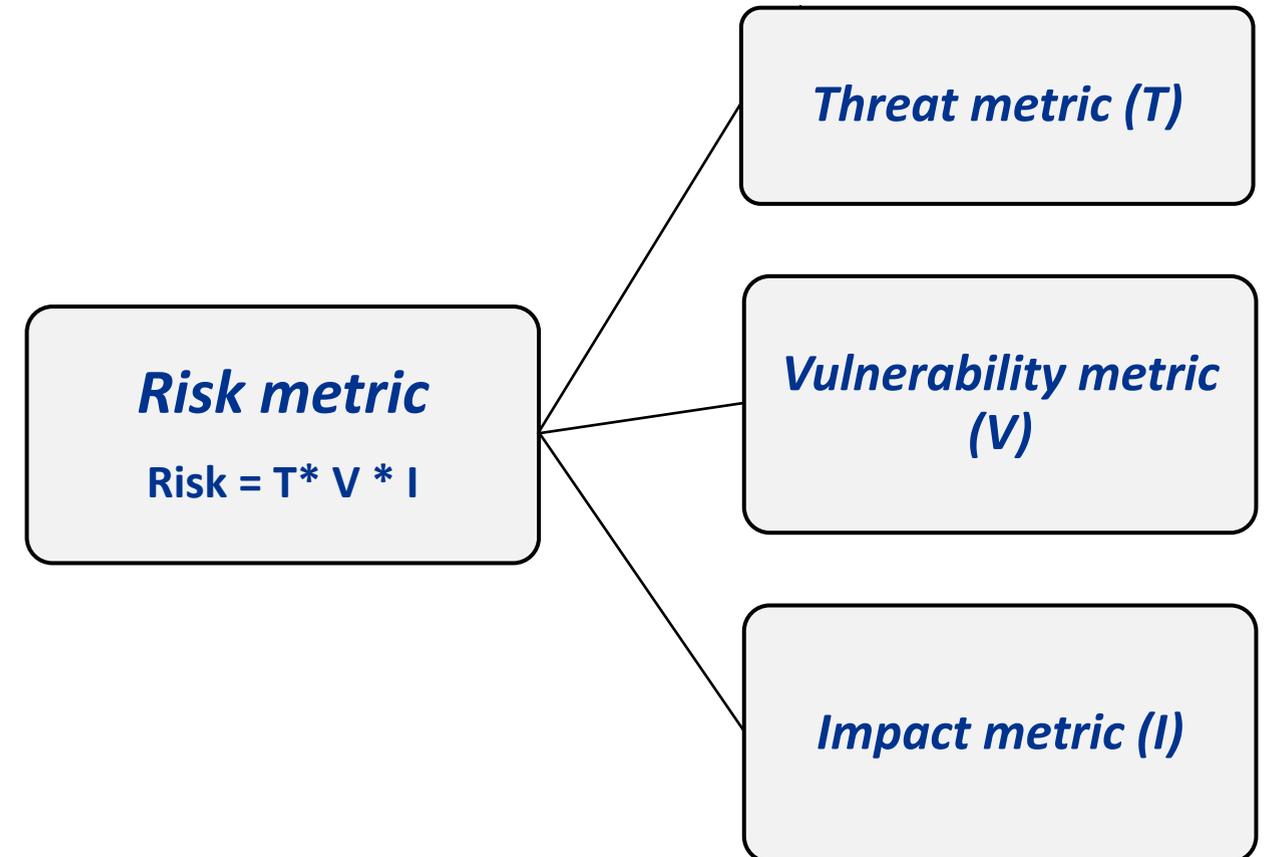


Image Source: <https://www.shutterstock.com/image-photo/wifi-smart-plug-on-white-background-1805313235> Last Accessed: 03/13/2022



Risk-Informed Approach

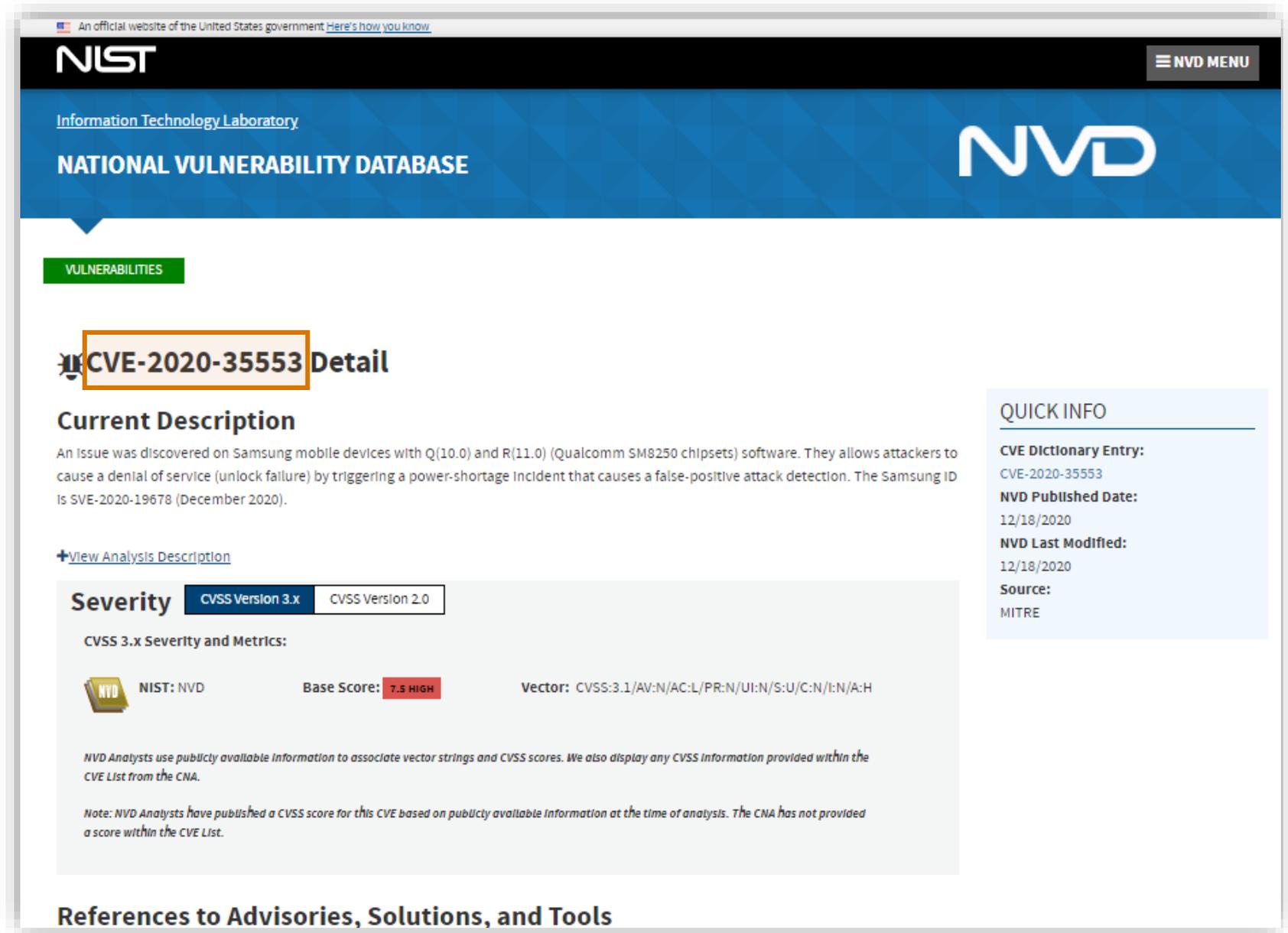
- *Risk* is potential loss or harm related to technical infrastructure, use of technology or reputation of an organization due to exposure or loss resulting from a cyber attack or data breach on organization
- *Risk metric* measures extent to which vulnerabilities in a product could be exploited or triggered by an adversary
- Why do we need *risk-metric*?
 - Basis for proactive security
 - Risk-informed prioritization of V&V
 - Efficient utilization of resources



Glyn A. Holton (2004) Defining Risk, Financial Analysts Journal, 60:6, 19-25, DOI: [10.2469/faj.v60.n6.2669](https://doi.org/10.2469/faj.v60.n6.2669)

Introduction to Common Vulnerabilities and Exposures (CVEs)

- Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities
- CVE ID is a unique, alphanumeric identifier referencing a specific vulnerability



The screenshot shows the NIST National Vulnerability Database (NVD) detail page for CVE-2020-35553. The page is titled "NIST Information Technology Laboratory NATIONAL VULNERABILITY DATABASE NVD". The main heading is "VULNERABILITIES" and the specific entry is "CVE-2020-35553 Detail".

Current Description
An issue was discovered on Samsung mobile devices with Q(10.0) and R(11.0) (Qualcomm SM8250 chipsets) software. They allows attackers to cause a denial of service (unlock failure) by triggering a power-shortage incident that causes a false-positive attack detection. The Samsung ID is SVE-2020-19678 (December 2020).

Severity (CVSS Version 3.x selected)
CVSS 3.x Severity and Metrics:
NIST: NVD Base Score: 7.5 HIGH Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

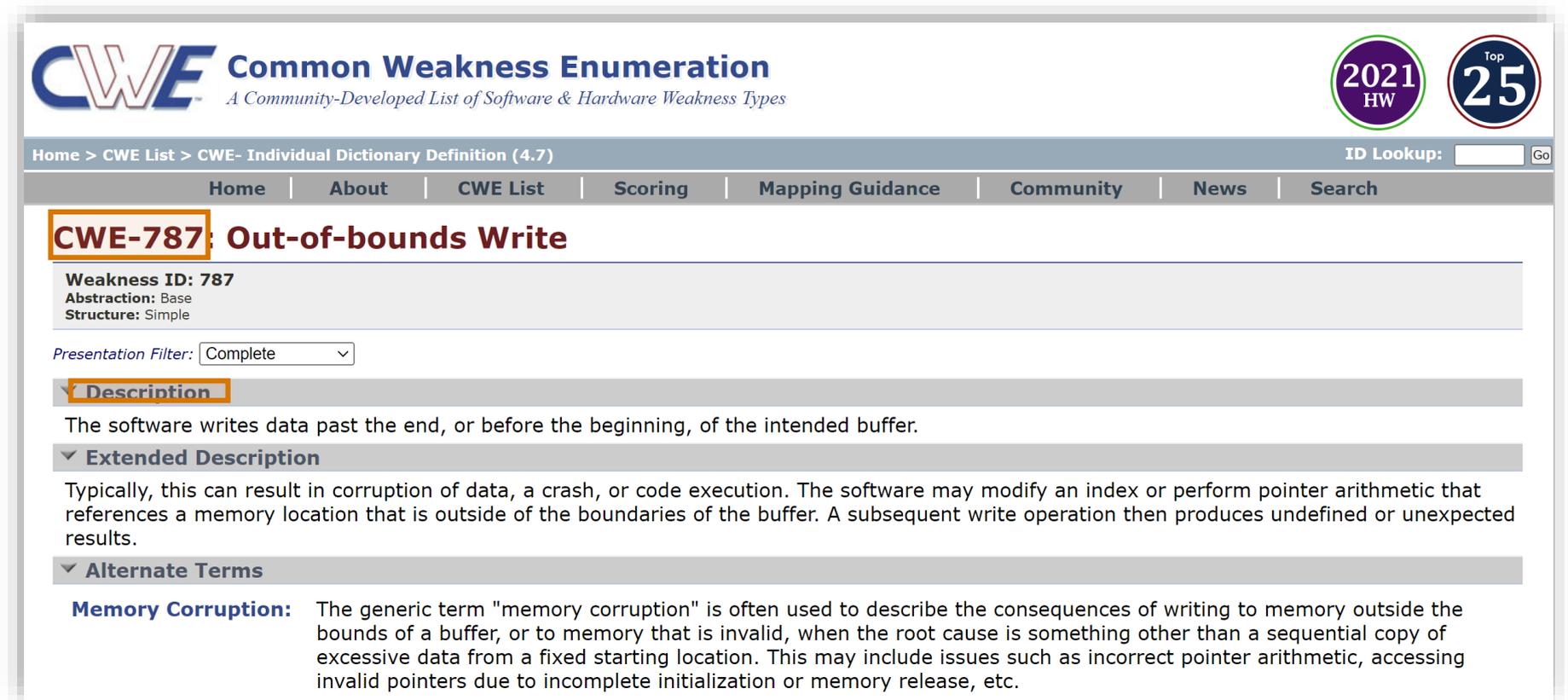
QUICK INFO
CVE Dictionary Entry: CVE-2020-35553
NVD Published Date: 12/18/2020
NVD Last Modified: 12/18/2020
Source: MITRE

References to Advisories, Solutions, and Tools

Source: <https://nvd.nist.gov/vuln/detail/CVE-2020-35553>

Introduction to Common Weakness Enumeration (CWE™)

- Formal list or dictionary of common *software and hardware weaknesses* that can occur in architecture, design, code, or implementation that can lead to exploitable security vulnerabilities
- Includes *Weakness ID, description, applicable platforms, common consequence* and other relevant information



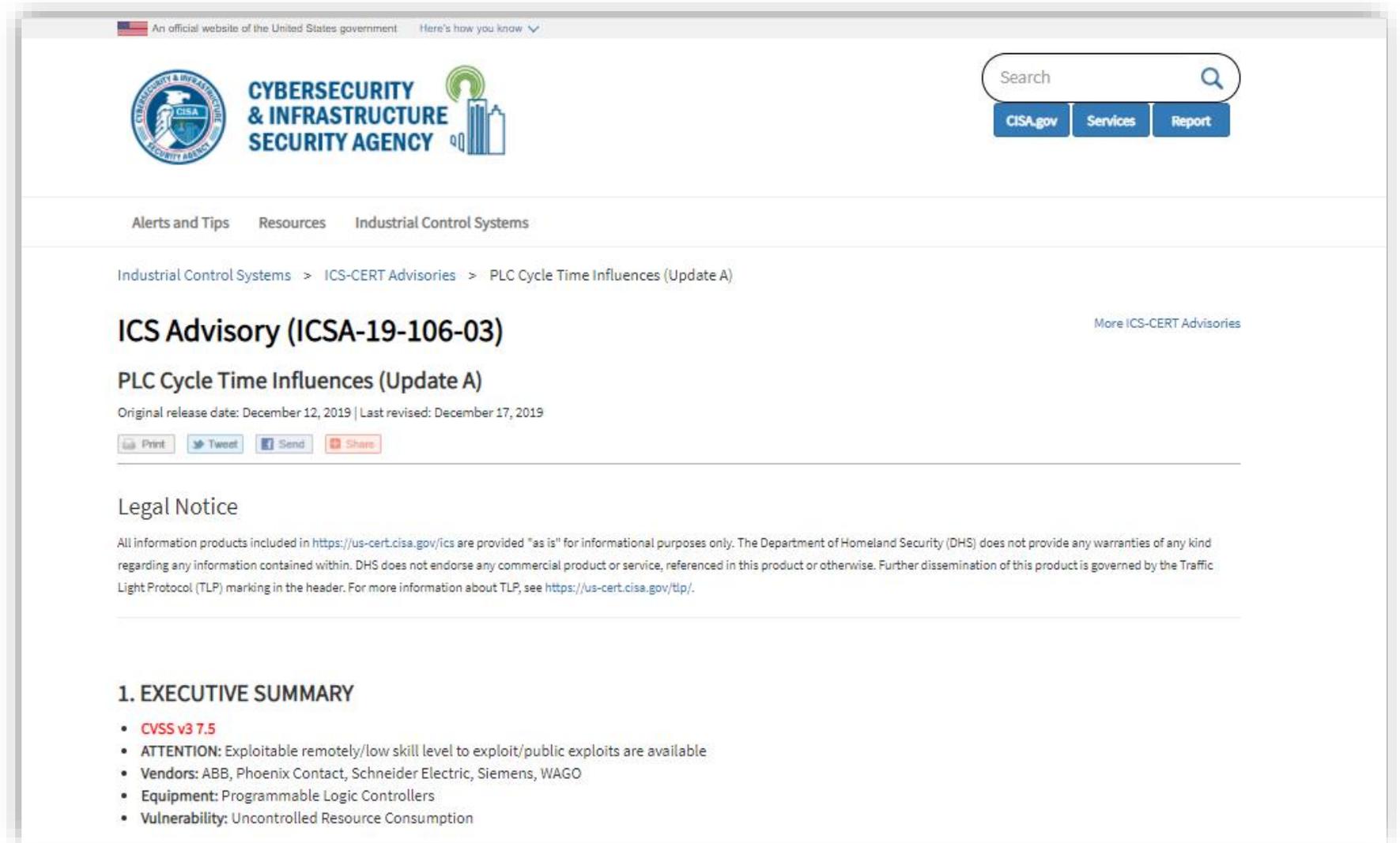
The screenshot shows the website for the Common Weakness Enumeration (CWE). The header includes the CWE logo and the text "Common Weakness Enumeration - A Community-Developed List of Software & Hardware Weakness Types". There are also two circular badges: "2021 HW" and "Top 25". The navigation bar includes links for Home, About, CWE List, Scoring, Mapping Guidance, Community, News, and Search. The main content area is titled "CWE-787: Out-of-bounds Write" and includes the following information:

- Weakness ID:** 787
- Abstraction:** Base
- Structure:** Simple
- Presentation Filter:** Complete
- Description:** The software writes data past the end, or before the beginning, of the intended buffer.
- Extended Description:** Typically, this can result in corruption of data, a crash, or code execution. The software may modify an index or perform pointer arithmetic that references a memory location that is outside of the boundaries of the buffer. A subsequent write operation then produces undefined or unexpected results.
- Alternate Terms:**
 - Memory Corruption:** The generic term "memory corruption" is often used to describe the consequences of writing to memory outside the bounds of a buffer, or to memory that is invalid, when the root cause is something other than a sequential copy of excessive data from a fixed starting location. This may include issues such as incorrect pointer arithmetic, accessing invalid pointers due to incomplete initialization or memory release, etc.

Source: <https://cwe.mitre.org/data/definitions/787.html>

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Advisory

- Conduct vulnerability and malware analysis
- Provide situational awareness in the form of actionable intelligence
- Coordinate the responsible disclosure of vulnerabilities/mitigations

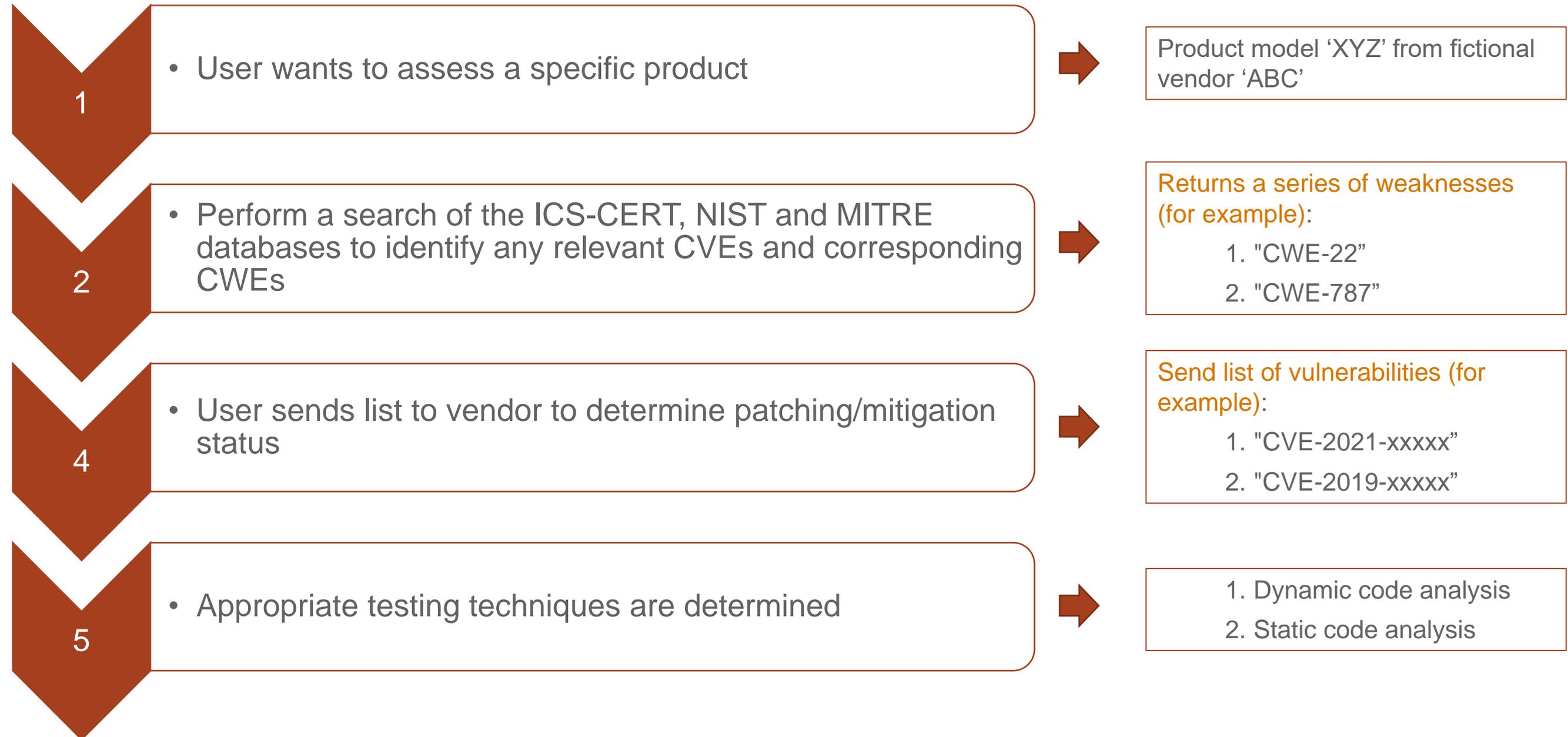


The screenshot shows the official website of the Cybersecurity & Infrastructure Security Agency (CISA). The page is titled "ICS Advisory (ICSA-19-106-03)" and "PLC Cycle Time Influences (Update A)". It includes a search bar, navigation links for "Alerts and Tips", "Resources", and "Industrial Control Systems", and a breadcrumb trail: "Industrial Control Systems > ICS-CERT Advisories > PLC Cycle Time Influences (Update A)". The advisory text includes a "Legal Notice" and an "EXECUTIVE SUMMARY" with the following bullet points:

- **CVSS v3 7.5**
- **ATTENTION:** Exploitable remotely/low skill level to exploit/public exploits are available
- **Vendors:** ABB, Phoenix Contact, Schneider Electric, Siemens, WAGO
- **Equipment:** Programmable Logic Controllers
- **Vulnerability:** Uncontrolled Resource Consumption

<https://www.cisa.gov/uscert/ics/advisories/ICSA-19-106-03>

Risk-Informed V&V Approach: Getting Started



Pre-Procurement Guidance



Lifecycle phases evaluated

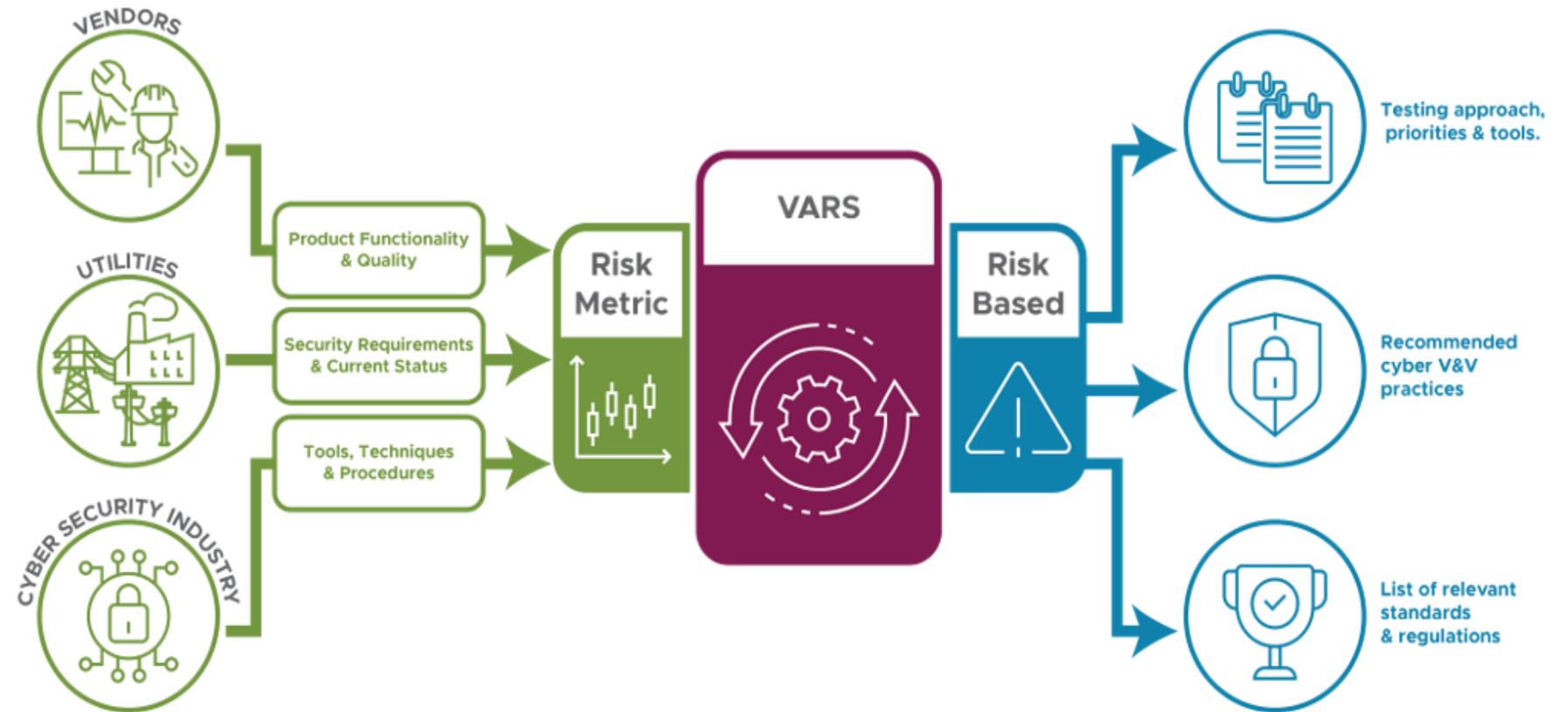
1. U.S. Department of Homeland Security (2009). [“Cyber Security Procurement Language for Control Systems.”](#) Accessed April 11, 2022
2. Energy Sector Control Systems Working Group (ESCSWG) (April 2014). [“Cybersecurity Procurement Language for Energy Delivery Systems.”](#) Accessed April 11, 2022:
3. “IEC 62443-4-2: Security for Industrial Automation and Control Systems, Part 4-2: Technical Security Requirements for IACS Components”
4. “IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities,” in IEEE Std 1686-2013 (Revision of IEEE Std 1686-2007), vol., no., pp.1-29, 13 Jan. 2014.
5. “NATF Supply Chain Security Criteria Version 2.0”, Accessed April 11, 2022: <https://www.natf.net/industry-initiatives/supply-chain-industry-coordination>

Product-specific information and vendor organizational level practices together determine security maturity

Risk-Informed Verification and Validation Recommendation (RIVVR)

RIVVR tool for organizations to determine risk-informed Verification and Validation (V&V) approaches

- Tool will be ready for pilot testing by June 2022
- Target users:
 - Primary: Asset owners – Energy utilities
 - Secondary: Vendor & OEM – EDS hardware/software vendors, integrators



Weaknesses to Techniques to Standards and Tools

STANDARDS

IEEE 1686-2013
 IEEE 1012-2016
 IEEE C37.1
 IEEE C37.238-2017
 CIP-007-6
 CIP-010-3
 CIP-013-1
 ANSI/ISA-62443-2-4-2018
 ANSI/ISA-62443-4-1-2018
 ANSI/ISA-62443-4-2-2018
 NIST SP 800-30 Rev. 1
 NIST SP 800-82
 NIST SP 800-160
 NIST SP 1800-2
 API Standard 1164
 ...

Vulnerability / weakness example

- CVE-2019-xxx : Software has a Buffer Overflow in the IPv4 component.
- CWE-787 (Out of Bounds Write)



V&V techniques

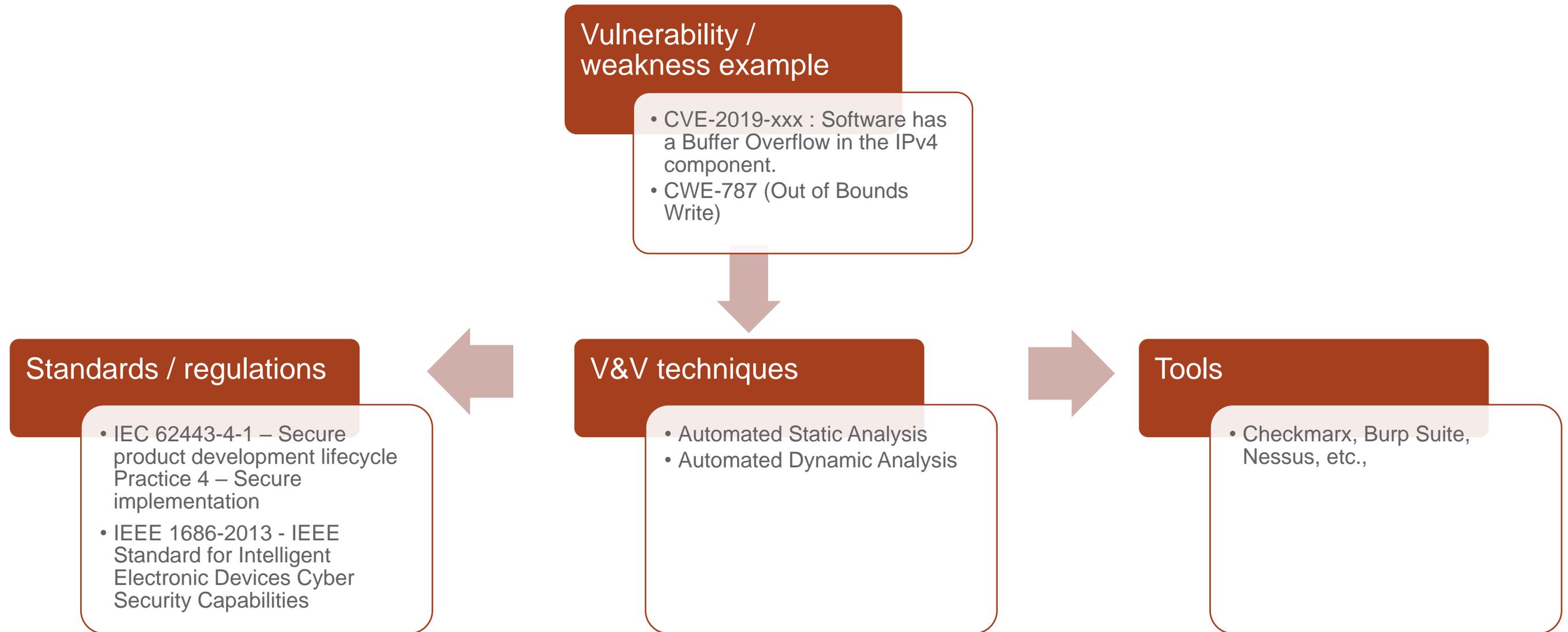
- Automated Static Analysis
- Automated Dynamic Analysis

TOOLS

AMD CodeAnalyst
 Checkmarx
 FlawFinder
 Ghidra
 GNU Debugger
 Lint
 Metasploit Framework
 MOPS
 Nmap
 RATS
 SonarQube
 SSASS-E
 Tenable Nessus
 WhatsUp Gold
 ...

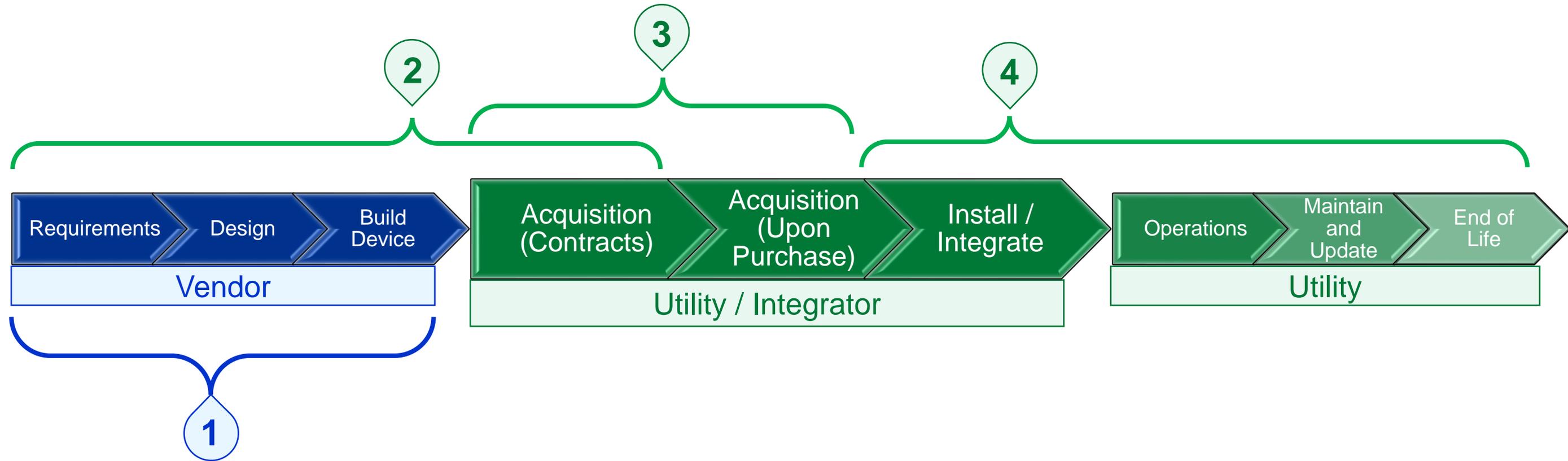
Recommendations of V&V prioritized according to risk type

Weaknesses to Techniques to Standards and Tools



Recommendations of V&V prioritized according to risk type

Major Benefits



- 1 Standards, techniques and tools for vendors
- 2 Pre-procurement guidance checklist for utilities
- 3 Risk scoring for resource prioritization/planning/replacement
- 4 Standards, techniques and tools for utilities

Thank You

Risk-informed V&V recommendation (RIVVR) web-tool					
Relevant vulnerabilities, patches, V&V testing results	Risk-score based reasoning and prioritization of V&V testing	Recommended V&V testing approaches	Relevant standards/guidance and available tools		
		VARs Risk-informed V&V framework			
Pre-purchase guidance checklist for Cybersecurity V&V		Scoring of Risk metric for relevant weaknesses and vulnerabilities			
Vendors – Testing approaches, Security features	Utilities – Cyber Architecture, Security Controls	Cybersecurity & Threat intel community – Vulnerabilities, Weaknesses, Attack TTPs			

Seemita Pal
seemita.pal@pnnl.gov