NSA CYBERSECURITY

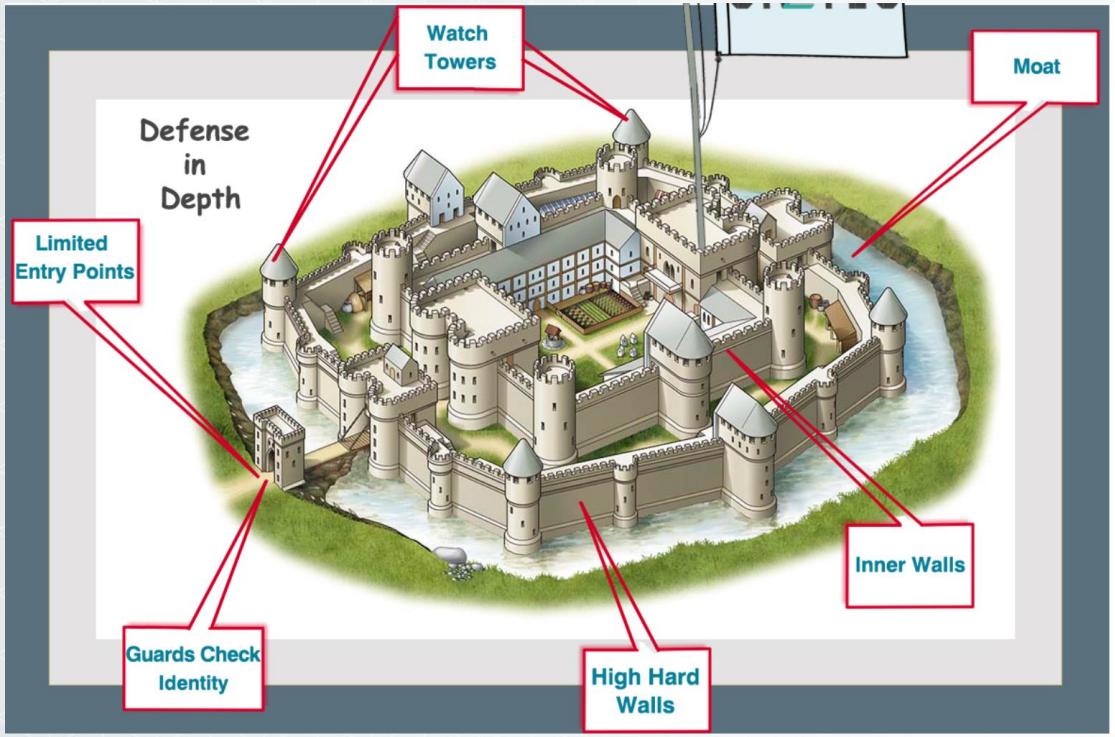
Software Security and SBOM

Dr. Jade Stewart, NIAP Portfolio Manager
jgstewa@niap-ccevs.org

Crypto Module Bootcamp at Concordia University

Feb 27, 2024

Architecture



Past: Traditional Security – preventive

- On-premise

Prevent by good Software Security

Present (perimeter-less)

- Cloud
- IoT

Prevent & Detect by enhancing Software Security and using Zero Trust

Attackers pick easy vulnerabilities; now using AI

Software Security (1 of 2)

- Needs to be designed in at the beginning of the project and not added at the end
  - Cost & time saving
- Utilize Secure Coding Principles
- Testing Techniques
  - Static Code Analysis
  - Dynamic Code Analysis – test a running application for exploitable vulnerabilities (during development)

    Also called Dynamic Application Security Testing
  - Fuzzing – input data “fuzz” to try to crash software or break thru defenses
  - Can use AI
  - Automated Security Scanning (to check for known vulnerabilities)
  - Penetration Testing (can be both static & dynamic), usually manual, post development
- Key Coding Standards: OWASP, CERT, DISA STIG, ISO Standards, e.g., 5055
- Catalogs of security vulnerabilities & exposures: CWE, CVE, NVD, KEV

Software Security (2 of 2)

- Needs to cover the Software Development Lifecycle (SDLC)

  Development & Deployment (includes testing). ISO/IEC 12207 standard
- Executive Order (EO) 14028 May 2021 on Improving the Nation's Cybersecurity assigned NIST to develop new standards, tools, best practices & other guidelines to enhance software supply chain security: https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity
  - Evaluation of software security
  - Security practices - developers & suppliers
  - Demonstration of conformance with secure practices
  - Labeling of consumer software to inform customer
- Secure Software Development Framework (SSDF) produced by NIST (SP 800-218) – catalog of practices
- Software Bill of Materials (SBOM) – Defined in EO 14028 10(j)

What is NIAP?

National Information Assurance Partnership https://www.niap-ccevs.org

Information Assurance = Cybersecurity

- NIAP is responsible for
  - the U.S. implementation of the Common Criteria
  - Managing the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) validation body
- NIAP manages a national program for developing Protection Profiles and evaluation methodologies
- NIAP certifies products (CCTL/vendor submits a Security Target document for the Target of Evaluation):

  https://www.niap-ccevs.org/Product/PCL.cfm
- NIAP partners with NIST
  - Approval of Common Criteria Testing Laboratories
  - Utilizes NIST's Cryptographic Algorithm Validation Programs and crypto algorithm documentation

    https://www.nist.gov/programs-projects/cryptographic-algorithm-validation-program

    https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/validation-search

CNSSP 11

- NIAP operates under the authority of the Committee on National Security Systems Policy 11 (CNSSP-11, a national policy governing the acquisition of information assurance (IA) and IA-enabled information technology products, Published 2013 (currently being updated)
  - https://www.cnss.gov/CNSS/issuances/Policies.cfm Policy 11
  - Clarifies that NIAP is the designed program to implement and administer a process governing the testing and evaluation of COTS IA and IA-enabled IT products required evaluation processes applicable to Commercial-Off-the-Shelf (COTS).
  - "The Director, NSA is responsible for implementing NIAP as it applies to National Security Systems to include approving processes for the evaluation of COTS products when they are to be used to protect information on the NSS."
  - Processes & procedures in policy are to reduce risk of compromising the NSS and the information contained therein
    - Ensure security-related features perform as claimed
    - Ensure the security evaluations produce achievable, repeatable & testable results
    - Promote cost effective and timely evaluations
- https://www.nsa.gov/Portals/75/documents/resources/everyone/2023-02-NIAP_brochure_trifold_1.pdf?ver=6uZYb3Lc3f8836n4M3t-oA%3D%3D

What is the Common Criteria?

The **Common Criteria for Information Technical Security Evaluation** (CC, ISO 15408) Parts 1 – 5 and the companion **Common Methodology for Information Security Evaluation** (CEM, ISO 18045) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA)

https://www.commoncriteriaportal.org

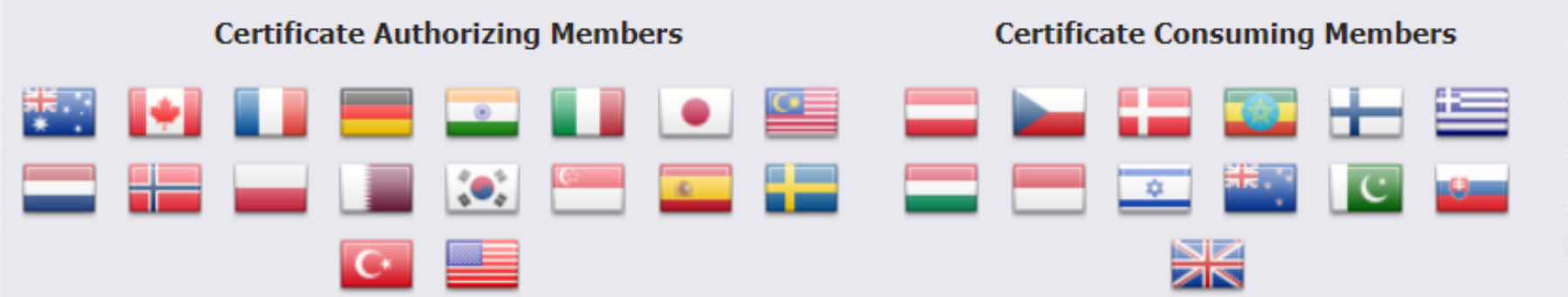
Currently developed and published by ISO/IEC JTC 1/SC27 Information security, cybersecurity and privacy protection (Working Group 3 Security Evaluation, Testing and Specification): https://committee.iso.org/home/jtc1sc27

https://www.commoncriteriaportal.org/cc/index.cfm

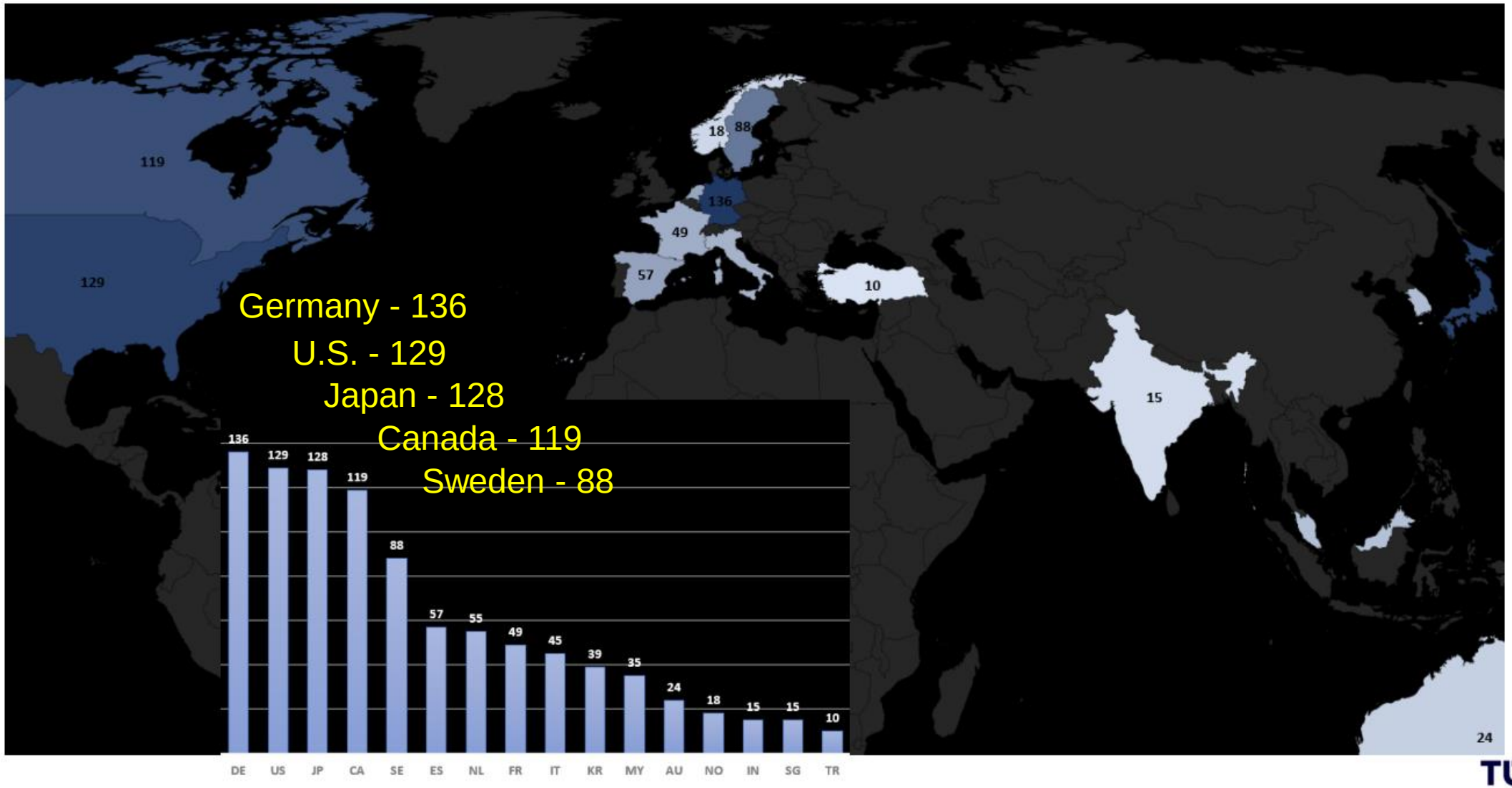
ISO Standards: https://www.iso.org/standards.html

- Internationally agreed, describing the best way of doing something "best practices"
- Distilled wisdom of people with expertise in their subject matter

CCRA Members



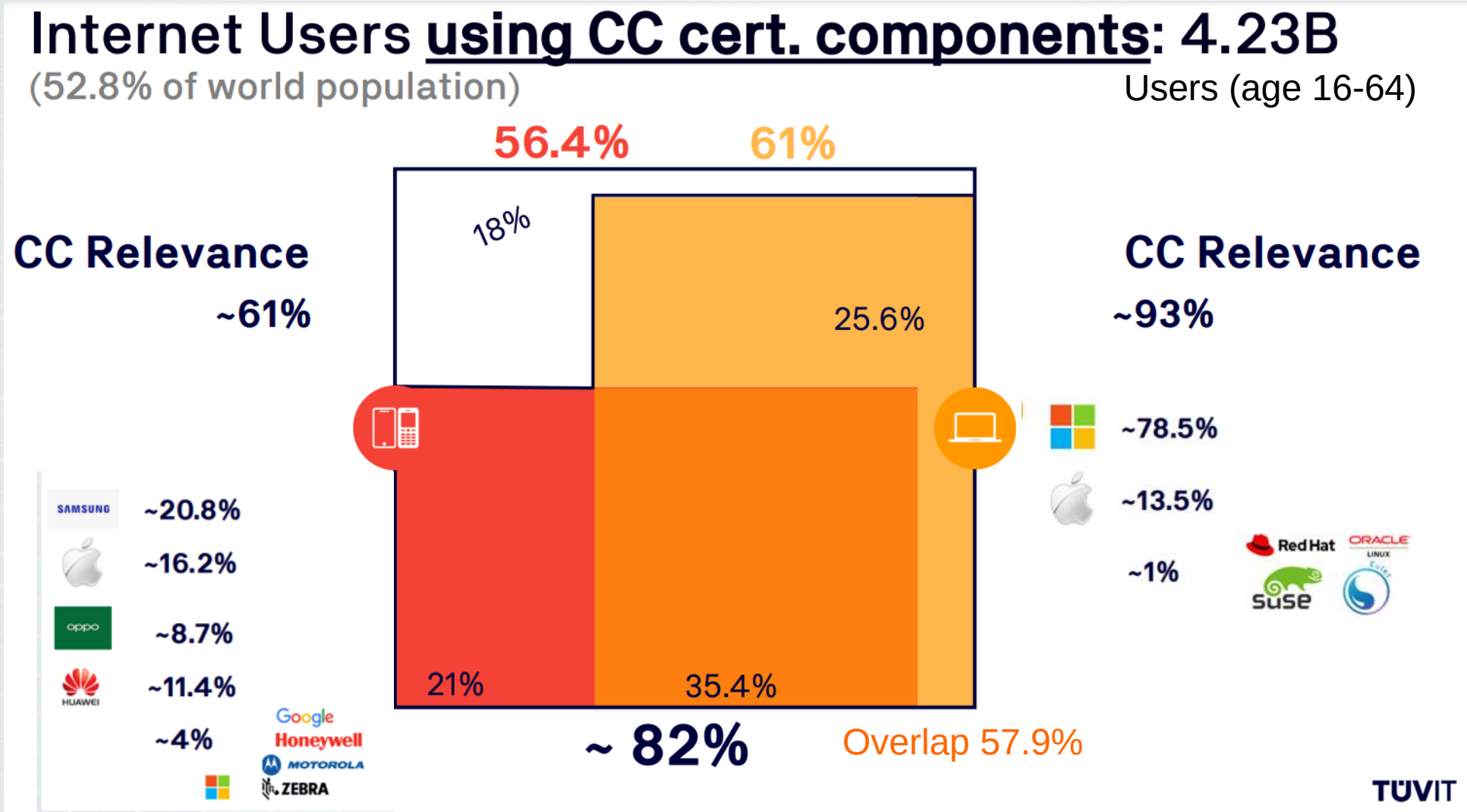
CC Certificates – no IC (~960) 2018-2022



TÜVIT

Presented by Markus Bartsch, TUVIT at the EU Cyber Act Conference 2023

Statistics: Usage of Products with CC Certified Components



An estimated
4.2 billion people
53% of world population
use CC certified components

Data only looking at internet usage:
- mobile phone 92.3%
- laptop/desktop 65.6%

Total internet users: 5.2 billion, 64.4% of world pop.

Presented by Markus Bartsch, TUVIT at the EU Cyber Acts Conference March 2023

Protection Profile Development Process

- In conjunction with Agency Stakeholders, a new Protection Profile is decided. Phases:
  - There must be Agency SMEs and at least two external vendors who will participate in a technical committee to write the PP
  - Phase 1: Agency SME in conjunction with NIAP writes the Essential Security Requirements (ESR), which contains items like use cases, resources to be protected, functionality requirements, assumptions, scope
  - Phase 2: A Technical Committee is formed
  - Phase 3: The TC defines the threats, security requirements and assurance activities. These activities dictate what is to be described and testing
  - Phase 4: Approval for Public Release on NIAP Website
- When technical issues or questions arise, a technical query is submitted to NIAP.
  - The SME, Validators and NIAP discuss the query
  - This can result in a Technical Decision. Addressing TDs is required according to published date and the text is folded into the next version of the PP

NIAP Portfolio

Establish and implement processes to oversee COTS product evaluations under the terms of the Common Criteria Recognition Arrangement to ensure evaluated COTS IT products are available for use in NSS and worldwide.

~51 Protection Profiles (PPs), PP Modules or Packages

Some International ones cPPs

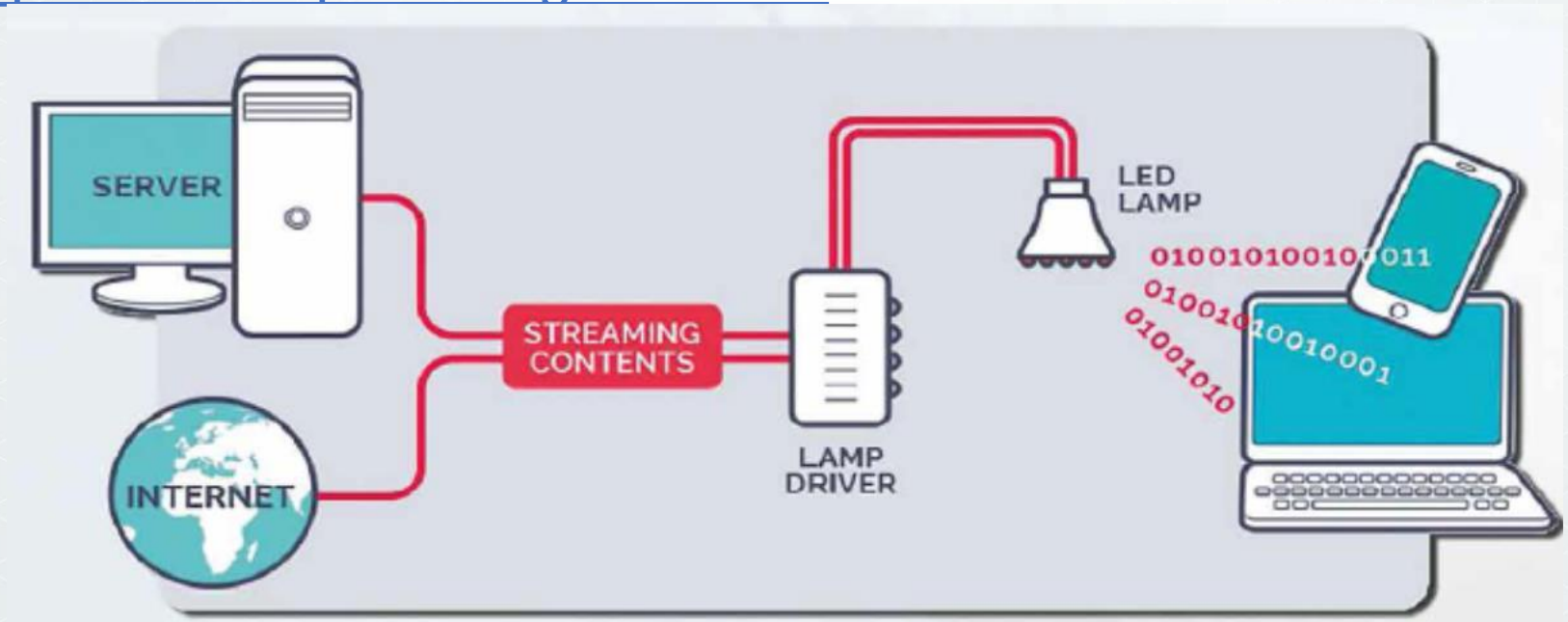
https://github.com/commoncriteria

Protection Profile Development Hot Off the Press

LiFi (Light Fidelity) PP will start in Spring 2024

LiFi is a wireless communication technology which utilizes light to transmit data and position between devices. Introduced at a TedGlobal talk in 2011

https://en.wikipedia.org/wiki/Li-Fi



Implementation of LiFi

https://www.led-professional.com/resources-1/articles/lifi-what-it-is-how-it-works-what-it-provides-how-to-apply-and-its-future-prospects

Protection Profile Updates

- NIAP is updating Protection Profiles to be compliant with CC:2022
  - Deadline Dec. 2025
  - https://www.niap-ccevs.org/Profile/PP.cfm
- NIAP PPs must be compliant with CNSA 1.0, which specifies the approved NIST cryptographic algorithms approved. Algorithms are in CNSS Policy 15 Appendix B. https://www.cnss.gov/CNSS/issuances/Policies.cfm
- NIAP PPs must start to adhere to CNSA 2.0 – algorithms designed for protection against a future deployment of a cryptanalytically relevant quantum computer (post-quantum cryptography)

  https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

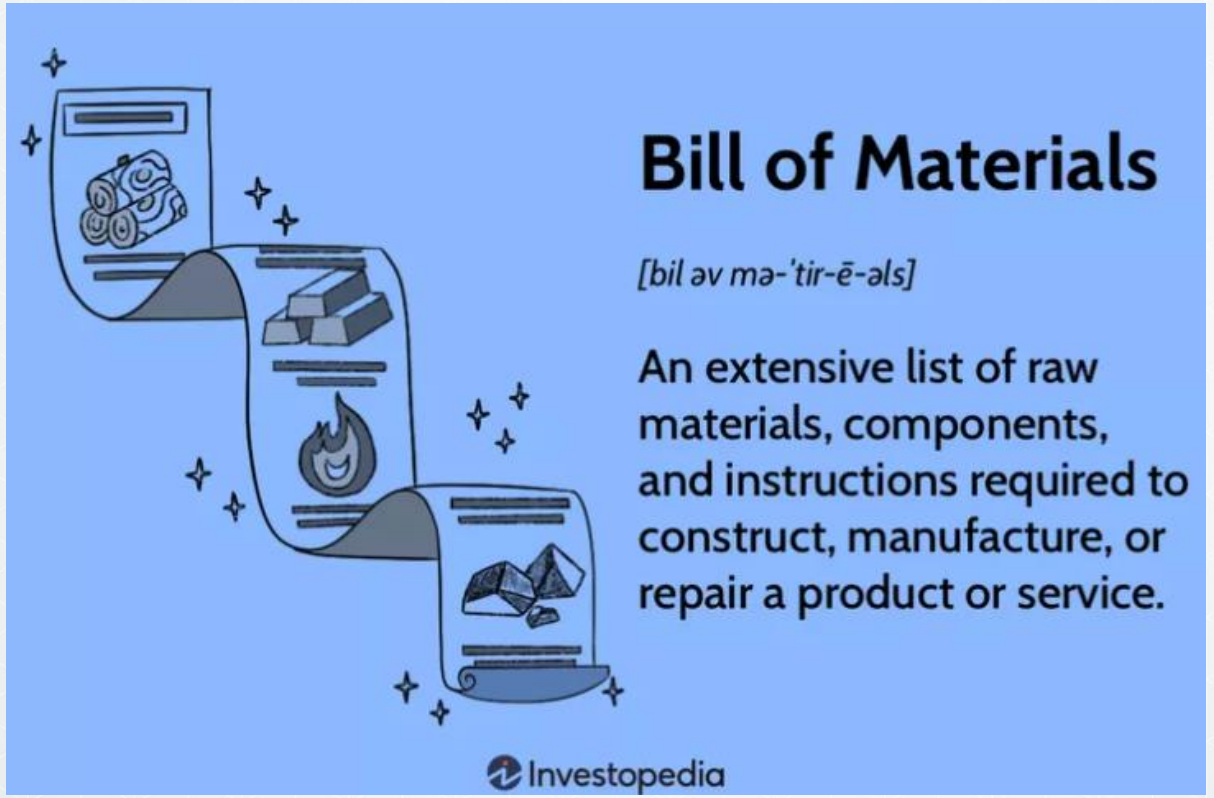
CCTL Evaluations

- Vendor/CCTL submits product in a Security Target document; describes the Target of Evaluation
- The CCTL performs the Evaluation Activities listed in the Protection Profiles
  https://www.niap-ccevs.org/Profile/PP.cfm
- There must be exact conformance to the PPs, Modules and Packages
- The Validators review the CCTL package submitted to NIAP
- Successful => Posted on NIAP's Product Compliant List (PCL)

Dilbert on Quality; CCTL evaluate the vendor's submissions

SBOMs: What is an SBOM

- Software Bill of Materials. There is also HBOM – Hardware BOM and people have defined multiple other types.
- NIAP is currently focusing on SBOM, based on Executive Order 14028 in 2021.



https://www.investopedia.com/terms/b/bill-of-materials.asp

Why SBOM – Current Status

- SBOMs or attestations mandated as part of the federal acquisition process in the near future
  - FDA requiring SBOMs as of October 1, 2023: Commercial, SOUP and off-the-shelf
    - SOUP = Software of Unknown Provenance
  - Attestations or secure software three months (for critical software) after the CISA common form finalized by CISA and approved by OMB (M-22-18 Enhancing Software Security), M-23-16 Update
    - Comments accepted thru Dec 18, 2023: https://www.cisa.gov/secure-software-attestation-form
  - Attestations only from the producer of the software end product (not underlying suppliers)
- NIAP needs to explore the use of SBOMs since NIAP certifies products for use on National Security Systems (critical products) and tracks vulnerabilities to products on the PCL.

SBOM Pilot for AppSW and the future AppSW cPP starting March 1st

- Comment on NIAP draft policy ended Dec 8. Review presented Feb 22, 2024

Why SBOM – Reasons

- **Software transparency**: SBOMs provide a list of ingredients used in the creation of a piece of software, such as open source software, components, and potentially even build tools. This enables producers and consumers to better inventory and evaluate license and vulnerability risk.

- **Software integrity**: While code signing is still the industry standard for trusting software and its integrity, SBOMs contain package and file checksums to enable consumers to validate the hashes, which can be useful in scenarios when signatures aren't present.

- **Software identity**: When vulnerabilities (CVEs) are created, they are assigned to a Common Platform Enumeration (CPE) identifier (or PURL), which can have issues attributing a CPE to a specific piece of software. Software IDs within SBOMs provide a much more accurate way to identify software.

  https://devblogs.microsoft.com/engineering-at-microsoft/generating-software-bills-of-materials-sboms-with-spdx-at-microsoft/

- Important for NIAP:
  - Transparency
  - Identity
  - Integrity in some cases

EO 14028 (May 2021)

- Director of NIST tasked to issue guidance for practices that enhance the security of the software supply chain. The guidance shall include standards, procedures, or criteria regarding:

  … Sec 4. Enhancing Software Supply Chain Security

  … (e.vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website

  … (e.viii) participating in a vulnerability disclosure program that includes a reporting and disclosure process

  … (e.x) ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion of a product.

  … (f) Secretary of Commerce in coordination with … National Telecommunications and Information Administration (NTIA) shall publish minimum elements for an SBOM

  … (g, i, j and k) critical software defined and guidance outlining security measures for critical software defined. Agencies need to comply.

- More guidance issued since then: M-21-30, M-22-16, M-22-18. NIST Software Supply Chain Security Guidance (lists SBOM and participating in a vulnerability disclosure program).
- Summary: agencies will be requiring SBOMs.
- NIAP can use SBOMs for vulnerability tracking and possibility checking during the validation process.

SBOMs for NIAP: Overview

- Software Bill of Materials (SBOM) - Executive Order 14028 (May 2021): https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
  - Supply Chain Vulnerabilities (e.g., Log4j, Solarwinds)
    - NIST Secure Software Development Framework (SSDF) catalog has SBOM - SP 800-218
- Memorandum M-22-18 Sept 2022: https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf
  - SSDF and NIST Software Supply Chain Guidance (has resource links)
- NIAP Motivation: The Situation: Vulnerabilities
  - Vulnerability Overview
  - NIAP Policy Letter #17
    - https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/policy-ltr-17-update2.pdf
  - Need to Easily Know if there are vulnerabilities – currently a manual process.
- March 2023 - ENISA has Rated Supply Chain Risk Management as top emerging cybersecurity threat for 2030: https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030
- Sept 2023 - CISA released HBOM guidance. (Note: NIAP will not be utilizing HBOM for pilot)
- November 23: Enduring Security Framework Guidance on SBOMs: https://media.defense.gov/2023/Nov/09/2003338086/-1/-1/0/SECURING%20THE%20SOFTWARE%20SUPPLY%20CHAIN%20RECOMMENDED%20PRACTICES%20FOR%20SOFTWARE%20BILL%20OF%20MATERIALS%20CONSUMPTION.PDF

Software Bill of Materials (SBOM) History 1 of 2

- Definition: A formal record containing the details and supply chain relationships of various components used in building software
- May 21, 2021 EO 14028 Improving the Nation's Cybersecurity charted NIST with developing guidelines for security measures for critical software. SBOM should be provided to purchasers.
  - https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity
- July 12, 2021 National Telecommunications Administration (NTIA) defined the minimum elements for a Software Bill of Materials
  - https://www.ntia.doc.gov/report/2021/minimum-elements-software-bill-materials-sbom
  - https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf
- Aug 10, 2021 M-21-30 Protecting Critical Software through Enhanced Security Measures: "The Federal Government's ability to perform its critical functions depends upon the security of its software. Much of that software is commercially developed through an often-opaque process that may lack sufficient controls to prevent the creation and exploitation of significant application security vulnerabilities."
- https://whitehouse.gov/wp-content/uploads/2021/08/M-21-30.pdf
- Feb 4, 2022 – NIST produces software supply chain security guidance: https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf
- Feb 6, 2022: NIST identified consumer labeling in a document: *Recommended Criteria for Cybersecurity Labelling of Consumer Software*: initial information added May 8, 2022
- May 5, 2022: NIST published Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations SP-800-161 Revision 1 – discusses SBOM

Software Bill of Materials (SBOM) History 2 of 2

- July 22, 2022 M-22-16 Federal agencies are required to establish formal Supply Chain Risk Management programs for their own acquisitions. Agencies should target resources to appropriately track supply chain investments.
- Sept 14, 2022 M-22-18 Memorandum for Enhancing the Security of the Software Supply Chain through Secure Software Development Processes - requiring NIST to issue guidance and agencies to be required to comply with the Guidance: https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf
  - NIST Guidance
    - NIST Secure Software Development Framework (SSDF) SP 800-218
    - NIST Software Supply Chain Security Guidance: requires a SBOM and participating in a vulnerability disclosure program (from EO14028 Section 4e).
  - SBOMs may be required for critical software as defined in M-21-30 (August 10, 2021)
  - Attestation letters are required within 270 days of Sept. 14, 2022 (June 11th) – that includes critical software
  - M-23-16 Update changed attestation letter date to 6 months after OMB approval of **CISA** attestation common form
- Sept 18, 2022: Memorandum M-22-18 https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf
  - SSDF and NIST Software Supply Chain Guidance (has resource links). Firmware is considered part of Software.
- Senate Draft of Fiscal 2023 National Defense Authorization Act authorizes the Secretary of Defense to B
  - require SBOMs for "all non commercial software created for or acquired by the Department of Defense" and
  - To develop a plan for receiving SBOMs accompanying commercial software (to "understand promptly the cybersecurity risks to Department capabilities posed by discoveries of vulnerabilities and compromises in commercial and open source software"
  - It was reported that vendors successfully lobbied to drop this in Dec 2022 but... **SBOM requirements are on the way**
- Oct 2023 - FDA requires SBOMs

Vulnerabilities… Motivation for NIAP SBOM

- The **Java ECDSA vulnerability** CVE 2022-21449, rated high was brought to NIAPs attention. **April 2022:**
  - The Java Development Kit (JDK) version 17 and 18 contained a flaw in the ECDSA (Elliptic Curve Digital Signature Algorithm) signature validation making it trivial to digitally sign files and other data as if they were legitimate organizations. This could result in cryptographically signed downloads and bogus information.
  - The flaw was introduced when Oracle developers incorrectly converted the C++ algorithm to Java.
  - This vulnerability could affect some of 31 products that could use ECDSA. Required a manual analysis by NIAP.

CVE Rating 7.5 but some experts though it should be a 10

The Register

Oracle already wins 'crypto bug of the year' with Java digital signature bypass

- **OpenSSL vulnerability** CVE 2022-2074 High Severity **June 22, 2022**:
  - Serious bug in RSA for X86_64 CPUs supporting AVX512IFMA
  - could allow for remote code execution
  - fixed in OpenSSL 3.0.5
- **OpenSSL vulnerability** CVE 2022-0778 High Severity **March 15, 2022**:
  - Process has a bug that can cause it to loop forever when passing certificates that contain elliptic curve public keys for a certificate. Allows for Denial of Service (DoS) attacks
  - Fixed in OpenSSL 3.0.2

Vulnerabilities… Motivation for SBOM

- National Vulnerability Database (NVD) provides qualitative severity ratings in addition to the severity ratings from the Common Vulnerability Scoring System (CVSS)
- NVD Ratings (CVSS 2.0 only contained Low, Medium, High)

CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

- NVD contains Common Platform Enumeration (CPE) information for Software Bill of Materials (SBOM)
- Note: PURL is also being promoted as an identification scheme for all packages included in the document

NVD Example: CVE 2022-21449

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

CNA: Oracle **Base Score:** 7.5 HIGH **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

- **cpe:2.3:a:oracle:graalvm:21.3.1:*:*:*:enterprise:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:oracle:graalvm:22.0.0.2:*:*:*:enterprise:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:a:oracle:jdk:17.0.2:*:*:*:*:*:*:***
  Hide Matching CPE(s)
  - *cpe:2.3:a:oracle:jdk:17.0.2:*:*:*:*:*:*:**
- **cpe:2.3:a:oracle:jdk:18:*:*:*:*:*:*:***
  Show Matching CPE(s)

Some Vulnerability Databases:

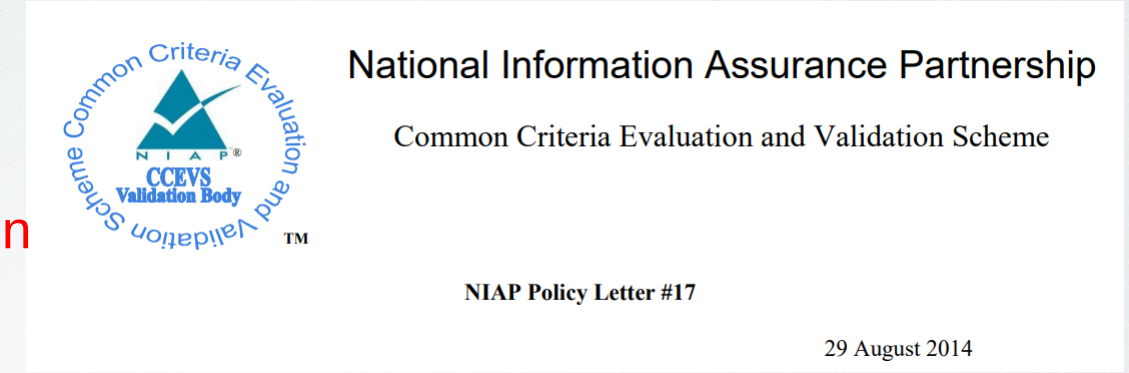
https://blog.adolus.com/what-is-vex-and-what-does-it-have-to-do-with-sboms

- National Vulnerability Database (NVD)
  - https://nvd.nist.gov/
  - Has API key
- Open Source Vulnerability Database (https://osv.dev)
  - Linux has 13,573 reported vulnerabilities
  - Android has 861
- CISA Known Exploited Vulnerabilities (KEV) Catalog
  - https://www.cisa.gov/known-exploited-vulnerabilities-catalog
  - Federal Civilian Executive branch agencies are required to remediate vulnerabilities
  - CSV Version and JSON version for download; email alerts
  - CISA - Vulnerability Exploitability eXchange (VEX) format for asserting the status of specific vulnerabilities

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date
CVE-2014-0160	OpenSSL	OpenSSL	OpenSSL Information Disclosure Vulnerability	2022-05-04	The TLS and DTLS implementations in OpenSSL do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information.	Apply updates per vendor instructions.	2022-05-25

NIAP Policy Letter 17

Outdated (2014) - requires revision



National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

NIAP Policy Letter #17

29 August 2014

From: https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/policy-ltr-17-update2.pdf

POLICY: This policy is applicable to products included on the NIAP Product Compliant List. If a vulnerability is discovered before, during, or after an evaluation, NIAP may notify the company and require modifications in order for the Target of Evaluation (TOE) to remain on the Product Compliant List (PCL). Any such notification will be sent out to the company point of contact. In response to such notification, the company must:

1. Present evidence to the NIAP as to why such modifications are unnecessary;
    a. NIAP will determine if the company's rationale is sufficient to allow the product to be listed, or remain listed, on the PCL.
2. Present to NIAP the company's plan to address the identified vulnerabilities;
    a. NIAP will determine if the company's mitigation of vulnerabilities is sufficient to allow the product to be listed, or remain listed, on the PCL.
3. Request NIAP remove or not place the product on the PCL.

Companies are not doing this, so NIAP needs to do it

FPT_LIB_EXT.1 is a start but insufficient

- Analysis of the Java ECDSA crypto bug, demonstrated that the current methodology of finding software was insufficient (not a SBOM)
- VID 11067 Nessus Manager Appendix A: Platform APIs Under Linux:

Used by Nessus bug report generator:

uname, dmesg, tail, killall, sh, uptime, ls, ps, grep, xargs, netstat, arp, df, cat, tail, rpm, free, ifconfig, du, tar

What Linux distribution, what version?

- In the ST Appendix A: Platform APIs Third Party Libraries (bundled with product):

Apache FOP, chart.js, DataTables, expat, Flatiron Director, Font Awesome, GLYPHICONS, Handlebars, jemalloc, jQuery, jQuery Cookie, jQuery FileUpload, jQuery HotKeys, jQuery scroll.To, jQuery tipsy, jQuery UI, JSONSL, less.js, libbzip2, libjpeg, libpcap, libpcre, libxml2, libxmlsec, libxslt, List.js, moment, OpenSSL, SEE, Select2, Snappy, snprintf.c, SQLite, Underscore,js, WinPCAP, ZIPVFS, zlib

What version? Maybe even what build?

National Telecommunications and Information Administration (NTIA) Minimum Elements 2021

Minimum Elements	
Data Fields	Document baseline information about each component that should be tracked: Supplier, Component Name, Version of the Component, Other Unique Identifiers, Dependency Relationship, Author of SBOM Data, and Timestamp.
Automation Support	Support automation, including via automatic generation and machine-readability to allow for scaling across the software ecosystem. Data formats used to generate and consume SBOMs include SPDX, CycloneDX, and SWID tags.
Practices and Processes	Define the operations of SBOM requests, generation and use including: Frequency, Depth, Known Unknowns, Distribution and Delivery, Access Control, and Accommodation of Mistakes.

https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

NIAP needs to investigate practices and processes in more detail during pilot and evaluation sync sessions

Requested Fields for Pilot

NTIA Minimum Elements: Data Fields – Documenting baseline info about each component that should be tracked. Format SPDX or CycloneDX. Includes:

- Supplier
- Component Name
- Version of the Component
- Other Unique Identifiers… (including build)
- Dependency Relationship
- Author of SBOM Data
- Timestamp

More details in NIAP policy to be published

More investigation needs to be performed:
https://www.cisa.gov/sbom

Plus:

- Integrity of SBOM: Hash
- SBOM Component Data Types (exact requirements need to be added)
- Provenance will probably be required in successive phases (not currently in policy)
- SBOM updates will also have to be discussed.
- Dependencies - Transitivity–how far? 1. Software from A calls B (open source) which then calls some other SW from Company A)
  2. Software from A calls B. B has a known SBOM that is "trusted" – **SBOM Trust**
- VEX – may require for some items (investigate: https://www.cisa.gov/resources-tools/resources/when-issue-vex-information)

Some Final Notes NIAP SBOM Pilot

Vulnerability Reporting:

- Ideally in future, vendors will report vulnerabilities to NIAP (it may be government mandated to report)
- NIAP will track vulnerabilities by using a commercial SBOM tool (Cybeats SBOM Studio) which will match components (CPE or PURL) to CVE or other vulnerability designator
- Cybeats can be used for the required NIAP vulnerability search before posting on the Product Compliant List
- With Cybeats, continuous monitoring, NIAP will require vendors to fix anything listed on the KEV, and at least critical and high vulnerabilities.
- NIAP is reviewing vulnerabilities policies based on lab and validator concerns. Expect some updates in the Spring.

SBOM Pilot

- Begins March 1st
- To join NIAP SBOM distro list, send email to niap@niap-ccevs.org
- Update briefing, comment matrix with responses, updated policy and policy addendum, plus labgram will be sent to distro list later this week
- Some sample Cybeats provided SBOMs will be provided to distro list (may not be sufficient for NIAP)
- Will compare Cybeats results to CCTL/vendor CVE required search prior to posting
- Will be starting Common Criteria Users Forum Group
  - How should SBOM be added to ALC (Lifecycle) in the Common Criteria
  - Discuss issues in the pilot and items that might need to be added
  - Discuss issues in adding to other protection profiles