Recommendations on the Use of Software Bill of Materials in Aviation

AIA Civil Aviation Cybersecurity Subcommittee

Stefan Schwindt – WG Chair (GE Aerospace)

Sean Sullivan – WG Vice Chair (The Boeing Company)

SW Bill of Materials Working Group Membership:

Kathleen Finke	Astronautics
Rob Hood	Astronautics
Kanwal Reen	Collins Aerospace (Lead Author)
Stefan Schwindt	GE Aerospace
Steve Douglas	GE Aerospace
Doug Nichols	GE Aerospace
Michele Tumminelli	Gulfstream Aerospace Corporation
Sam Masri	Honeywell
Anup Raje	Honeywell
Laurel Matthew	The Boeing Company
Tom McGoogan	The Boeing Company

Executive Summary

Cybersecurity threats have been increasing across all sectors, and there is much interest by stakeholders to reduce risks in strategies to reduce risks. In response to these challenges, in 2021, the Biden Administration developed and released Executive Order 14028 "Improving the Nation's Cybersecurity," in which the White House directed that the "Secretary of Commerce […] shall issue guidance identifying practices that enhance the security of the software supply chain."

Among its other provisions, in Sec. 4 "Enhancing Software Supply Chain Security," EO 14028 emphasized the following related to the security and integrity for "critical software" – [or] "software that performs functions critical to trust":

- Maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and controls on internal and third-party software components, tools, and services;
- Providing a purchaser a Software Bill of Materials (SBoM) for each product;
- Participating in a vulnerability disclosure program that includes a reporting and disclosure process;
- Attesting to conformity with secure software development practices; and
- Ensuring the integrity and provenance of open-source software used within any portion of a product.

The civil aviation sector has a unique allocation of accountability and responsibilities that differs from other sectors and requires an appropriate approach. While the Executive Order's provisions are not required for operators at this stage, the intent of this paper is to lay out a multi-phased plan for how civil aviation will adopt and update its practices to develop and maintain Software Bill of Materials (SBoM) information, specifically for its critical aviation industry products and services in order to aid the ultimate goal of managing exploitable vulnerabilities and accelerating incident response.

This report is intended to provide recommendations to all aviation stakeholders, including government and regulatory agencies, aircraft operators, aircraft manufacturers, and their suppliers for how SBoMs and related vulnerability identification and management should be effectively and efficiently implemented and utilized within the civil aviation sector. This will include addressing needed updates to industry standards as well as developing new capabilities to maintain and share SBoM-related information rapidly across the industry to facilitate both vulnerability and incident response.

Table of Contents

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association
1000 Wilson Boulevard, Suite 1700 | Arlington, VA 22209-3928 | 703.358.1000 | www.aia-aerospace.org

1 Software Bill of Materials (SBoM)

1.1 Overview

An SBoM is a specifically formatted file that contains an inventory of all software components included in a software deliverable, an inventory of the dependencies of those software components, basic information about the software components, and identification of hierarchical relationships between software components. With the use of third-party and open-source software, the software supply chain has become increasingly complex, resulting in multi-tiered supply chains for most software components. SBoMs provide a mechanism for transparency within the supply chain, so that the parties who use, produce, and operate software with third-party components have a better understanding of the supply chain associated with the components. This has the added advantage of offering a better understanding of the cyber risk associated with the third-party software components being used, as well as the potential to assess the impact of known and newly emerging vulnerabilities.

1.2 Use Cases for SBoMs

In addition to software supply chain transparency, SBoMs have many uses for a particular product:

- Vulnerability Management: The primary use case for SBoM is to aid vulnerability management. Since SBoMs offer a catalog of software components, they provide a faster and automated means of identifying impacted products. As with other industries, SBoMs will help identify what software components exist, where there are vulnerabilities known for these software components, and support analyzing the criticality of these vulnerabilities for further actions.

- Incident Response: In the event of a security incident or a data breach affecting an organization, an SBoM can help to provide documented evidence and a trail of what went wrong, where, and how the incident may have affected other areas, systems, or versions.[1] If the reason for the incident can be narrowed down to exploitation of vulnerabilities in software, an SBoM provides a fast and potentially automated means of performing a read across, and identifying other systems that might be susceptible.

- Code Origin: It is important to understand the origin of code for several reasons. If code is derived from other code, it is important to know this heritage because vulnerabilities may have been inherited. Avionics tends to have custom code although this code may include inclusion of software libraries such as those provided by compilers, or it may have different iterations and modifications from other airborne and non-airborne products.

Understanding the origin and source of code used that is from external sources including open-source software allows assessment of the trustworthiness of the software. Some repositories have been compromised in the past and unfortunately can be expected to be compromised in the future. Using

[1] Panorays Blog Site: "How an SBOM Helps Assess Third-Party Security Risk", Dov Goldman, 6 July, 2023

code origin fields, organizations can monitor if they may have been exposed to such a compromise and unintentionally included malicious software.

For military projects, it may be necessary to monitor the country of origin of the software included. Maintaining code origin in SBoM can aid compliance with such requirements.

- Obsolescence Management: SBoMs provide a means to identify the third-party software components used. This information can be used to determine if the components are still supported by the producers of the software or by the open-source community in the case of open-source software.

- License Compliance: Since SBoMs provide a listing of third-party software in the least, they aid in understanding the license requirements for each of these components and can be used as a means of ensuring that licenses of the individual third-party components have not been breached.

1.3 Industry Status

1.3.1 EO 14028 Provisions relating to Software Security and SBoM for Industry

In Executive Order 14028 "Improving the Nation's Cybersecurity" (May 2021), the White House directed the "Secretary of Commerce acting through the Director of NIST […] shall issue guidance identifying practices that enhance the security of the software supply chain."

Among other provisions, the Executive Order emphasized the following related to the security of software for U.S. critical infrastructure:

- Maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and controls on internal and third-party software components, tools, and services
- Providing a purchaser a Software Bill of Materials (SBoM) for each product
- Participating in a vulnerability disclosure program that includes a reporting and disclosure process
- Attesting to conformity with secure software development practices; and
- Ensuring the integrity and provenance of open-source software used within any portion of a product

Additionally, the National Cyber Strategy released in March 2023 expanded on the importance of SBoMs as part of a larger strategy to further incentivize the adoption of secure software development practices. The Administration will encourage coordinated vulnerability disclosure across all technology types and sectors; promote the further development of SBOMs; and develop a process for identifying and mitigating the risk presented by unsupported software that is widely used or supports critical infrastructure. In partnership with the private sector and the open-source software community, the federal government will also continue to invest in the development of secure software, including memory safe languages and software development techniques, frameworks, and testing tools.

1.3.2 Minimal Elements

While work is ongoing, the SBoM implementation plan is being co-led by the Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), the Department of Commerce (DOC), and the National Telecommunications and Information Administration (NTIA) as directed in the Executive Order. As such, it appears the immediate focus is on establishing minimum elements to be implemented initially across all federal organizations to support basic SBoM functionality.

These minimum elements are currently defined as follows:

- Data Fields - Documents 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 - Supports automation, including via automatic generation and machine readability to allow for scaling across the software ecosystem. Data formats used to generate and consume SBoMs, to include SPDX, CycloneDX, and SWID tags.
- Practices and Processes - Defines the operations of SBoM requests, generation and use including frequency, depth, known unknowns, distribution and delivery, access control, and accommodation of mistakes.

While SBoM implementation for the civil aviation industry at large has not yet been directed as a regulatory requirement, AIA believes that civil aviation must move now to be in a position to meet both future compliance requirements as well as to be interoperable with federal government organizations and facilities that will be implementing these changes. AIA also considers significant industry benefits in maintaining SBoM level details in aviation systems and software to increase the speed and effectiveness of vulnerability management.

1.3.3 Prior Aviation Industry Comments Provided to NTIA from AIA (Defense Policy & Integration)

In June of 2021, the Aerospace Industries Association (AIA) offered a series of comments in response to the Acting Administrator of the NTIA request for comments on the minimum elements for a SBoM and what other factors should be considered in the request, production, distribution, and consumption of SBoMs.

In these recommendations, AIA indicated its support for the Open Web Application Security Project (OWASP) CycloneDX standard for SBoM generation, which partially aligns with the NTIA's currently published fifteen "minimum elements of an SBoM." While the CycloneDX standard supports these "minimum elements of an SBoM," all elements are not guaranteed to be present, depending on the source material. Various tools, programs, and services can be leveraged for the generation and manipulation of SBoM data.

Additionally, AIA offered the following three recommendations with accompanying suggestions regarding the questions published on general SBoM practices:

1. AIA recommended NTIA consider the broad scope of the digital domain whereas the cornerstones should be prioritized foremost to include assurance elements while also accounting for risk management and threat modeling.

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association
1000 Wilson Boulevard, Suite 1700 | Arlington, VA 22209-3928 | 703.358.1000 | www.aia-aerospace.org

- As such, AIA strongly advised against including a Vulnerability List in the data fields, specifically if a vulnerability list is the product of one or more vulnerability analysis efforts, not an SBoM.
- However, AIA stated the ability to exchange with a standard format for currently associated vulnerabilities against the SBoM is advisable, though the analysis and reporting of such concerns may be held in a separate location. Existence and status of vulnerabilities can change over time, with no guarantee or signal on whether the SBoM data is up to date.

2. Value Stream Mapping is an essential practice that should be used to demonstrate actionable capabilities, value in operations, and allocation of resources over static informative specifications.

- Expanding the NTIA SBoM minimal elements to include NIST software assurance activities, lessons learned and mitigations from previous experiences related to incidents to include damage assessments is critical to the overall software and cyber landscape.
- AIA recommend processes to support the objective use cases of vulnerability/weakness analysis, vulnerability and incident response, supply chain assessment, pedigree and integrity of the software product, and dependent elements include SBOM confidentiality and integrity.
- AIA also asserted that automation tools built within DevSecOps Software Factories (SWFs) can be used to generate supporting artifacts to accommodate frequent (e.g., daily) vulnerability status changes to part, or all, of a package and associated SBoM.

3. Software Engineering recognized processes, international standards, and related innovative concepts should be reviewed, analyzed, and considered before authoring U.S.-only standards.

- Since the digital scope is dynamic and not U.S.-specific, a digital bill of materials must function in international markets with operational assurances that extend across sectors.
- AIA recommended a lightweight SBoM specification, capable of achieving real-world use cases across vendors or suppliers. For example, AIA provided “CycloneDX,” a recognized risk-based open-source project developing the specification, implementations, and providing standards in XML, JSON, and Protocol Buffers, as well as a large collection of official and community supported tools that create or interoperate across financial services, manufacturing, government, software, and security firms.
- Modular open systems architecture is key in supporting assorted technologies such as Kubernetes container orchestration that drives modularity through containerized microservice architecture into deployed systems. Modular approaches can simplify testing and deployment, while enabling a hardware agnostic software solution across cloud providers that extends into embedded environments.

2 Aviation Ecosystem

2.1 Accountability and Responsibility for Defects in Aviation

Aviation – both civil and military – are atypical in terms of accountability and responsibility for defects, including vulnerabilities, for the reason that they are allocated differently.In most sectors, the owner and operator of an asset is responsible for maintaining it. The responsibility within aviation is shared with the Design Approval Holder (DAH) holding the relevant Type Certificate (TC). To obtain a TC, the DAH must demonstrate that their product is safe and secure at the time of the design. However, the obligation does

not end with certification. Under 14 CFR 21, the DAH is required to monitor their products for defects that can affect safety. When and where defects are found, the DAH must analyze these and provide a remediation in a timely manner appropriate for the severity of the defect. The operators of aircraft are obligated to operate and maintain aircraft according to the instructions issued by the DAH and not deviate from the design as approved in the TC. Where changes must be made to an aircraft to maintain safety, an Airworthiness Directive (AD) is issued mandating operators to implement technical and/or procedural fixes within a specified timeframe. Adherence to these ADs is monitored by the authorities. If operators fail to follow these mandates, the airworthiness of the aircraft is jeopardized.

As a safety-critical industry, the precautionary principle applies to all activities occurring in the aviation sector. With respect to handling changes in certified products, this translates into a need to understand the impact of all changes and to demonstrate that any modifications do not have a negative impact on safety. As a result, it is typical that changes to aircraft may take considerable time, money, and resources to implement and certify. Hence the best practice in Information Technology (IT) environment of applying all available patches at the first suitable time does not translate to the aircraft.

In the scope of aircraft and its systems, this necessitates the incorporation of vulnerability management processes which include understanding the system-level impact (safety, operational, nuisance, etc.) of a vulnerability discovered in a hardware or software component of a system and whether that vulnerability is exploitable in its environment. This would account for any existing mitigating or compensating measures that are already implemented in the architecture. For any exploitable vulnerabilities that have an impact on flight safety, technical and/or procedural countermeasures would need to be identified. While technical fixes may be slow in aviation, procedures for flight and maintenance crews can be updated relatively quickly.

2.2 Challenges for SBoM Use in Aviation

Some challenges exist for implementing SBoM in aviation, particularly if SBoMs should be used in a regulatory or compliance context. These challenges relate to accuracy in generating SBoM, liability for correctness of the SBoM and associated vulnerability activities, supplier requirements and responsibilities, and how to manage legacy products.

2.2.1 Impacts to Existing Industry Standards

Airborne software is developed to meet RTCA DO-178B or C industry standards. Currently, these need to include a Software Configuration Index (SCI) listing that the software is delivered under an approval. When software is changed, the approval process requires an update of the SCI. The nature of change of the software would drive whether an SBoM would need to be created. Since it is not a required artifact, there is always a chance the software updates and SBoMs get disassociated. The existing software release process would hence need to be updated to require the generation of an SBoM as an artifact for software release. Assurance that SBoMs are current and valid can be obtained by auditing the adapted software process to ensure that an SBoM is an associated artifact for all software.

Additionally, the current International Aerospace Quality Group's AS9115A "Requirements for Aviation, Space, and Defense Organizations - Deliverable Software" lists the following requirements for formal software baseline to be delivered as part of quality assurance, including:

- Specific source and executable code items by version;
- Support software;

- Build instructions;
- Associated software documentation for the specific release;
- Test procedures and results;
- Interfaces to other software products and to target computer hardware; and
- The development and target computer environments (hardware and software).

AIA recognizes since many of these industry standards are currently up for revision, this may also provide an opportunity to be more explicit about hardware/SBoM implementation and alignment with the direction the federal government is going for the aviation sector.

2.2.2 Long product lifecycles

Aircraft have long lifecycles that vastly exceed the lifetimes of typical software components. Aircraft are generally assumed to have a lifetime of 30 years whereas many software components may have lifecycles and lifetimes of less than five years. This leads to the issue of software obsolescence where software might be deployed without any support from the original manufacturer. There may not be alternative software that can be integrated into the aircraft due to constraints on functionality or the capabilities of the processing hardware onboard. Otherwise, the time and capital cost of replacing software may delay adoption or even prohibit a change. However, obsolete software may pose a risk – patches no longer will be provided by the vendor for newly identified vulnerabilities or researchers may stop publishing vulnerabilities.

Obsolete software must be appropriately and continuously monitored to identify if there is sufficient protection against any known and unknown vulnerabilities from the software, and if any actions need to be performed. Organizations using third-party intellectual property (IP) may need to understand and incorporate processes in house to support risk-reduction activities on obsolete software components. SBoMs can support obsolescence management by not only comparing software components against known vulnerabilities, but also tracking supported and obsolete software components.

2.2.3 Accuracy

Success of vulnerability management using SBoM is based on the accuracy of the SBoM. As aircraft software does not undergo frequent changes, it may be difficult to determine if an SBoM has become stale or if no change has occurred. In IT environments, tools are often used to regenerate SBoM to have a comparison between actual and documented status as well as requiring periodic forced updates of SBoMs to ensure they are current.

Requiring periodic updates for SBoMs can significantly increase the cost of business without a corresponding gain in cybersecurity posture. Many suppliers have hundreds or even thousands of different versions of products implying that new documents need to be issued and distributed. The vast majority of products may undergo changes maximum at a rate of one per year, so frequencies higher than this would only produce cost. Use of tooling to generate an SBoM from deployed products is rarely possible as the avionics products do not support operating systems which could host such tools. These tools could interfere with functionality with a resultant safety impact and avionics typically would not have the capability to report out tool results.

The solution for maintaining the accuracy of SBoMs in aviation would be using the strict configuration management processes already in place.

2.2.4 Supplier requirements

Since SBoMs lead to more supply chain transparency, Commercial Off the Shelf (COTS) suppliers must be required to provide SBoMs as a part of the software documentation. This would require changes in the software procurement, associated deliverables, and suppliers either providing SBoMs for software deliverables or providing vulnerability information about the delivered software in a timely manner. This will also require considerations of obtaining SBoMs from the suppliers if they decide to stop supporting a particular software component.

Since SBoMs are dependent on the software supply chain, this requires a concerted effort by the industry to establish minimum expectations when it comes to vulnerability management of software components, as well as the use of industry standards for creation of SBoMs.

2.2.5 Legacy products

Due to the long lifetimes of aircraft, there is a high number of legacy products still in use. In the context of cybersecurity, these legacy products are aircraft that have been developed before cybersecurity special conditions or rules were in place. The legacy products are characterized by very limited connectivity. OEMs, and in particular the suppliers of avionics products, may have hundreds to thousands of differing product variations. Generation of SBoMs for legacy products pose a variety of issues: some SCIs may not be in electronic format or may not list the lower-level components. The use of software composition analysis tools to attempt to automatically generate SBoMs leads to unacceptable levels of false positives and false negatives.

The risk from legacy products can be considered low due to limited connectivity in the legacy architecture. SBoMs should be created on active products, and when software is updated or proactively in case there is a concrete suspicion that a vulnerability is present and exploitable. It is recommended that factors like the use of third-party IP, remote/wireless access functionality, and use of removable media, be used to prioritize legacy products for generation of SBoMs. This approach works well in aviation as any change to a certified product requires a rigorous process for managing the change, thus in the future it can include the generation or update of an SBoM and triggering a related vulnerability management activity.

2.3 Recommendations for aviation ecosystem

2.3.1 Expectations for the stakeholders

Independently, SBoMs are an input to the vulnerability management process that enables faster and more timely identification of issues.

The effective use of SBoMs by the various stakeholders is predicated by the establishment of the robust vulnerability management processes. The vulnerability management process should work independently of the use of SBoMs and incorporate mechanisms for ingesting vulnerability information for their components (hardware, software, etc.), performing a risk assessment and criteria for remediation efforts.

AIA recommends that organizations at every level deploy a vulnerability management process for products with documented methodologies for:

- Defining and cataloging the assets (products);
- Collecting vulnerability information about the assets;

- Establishing a risk assessment methodology, driving the urgency around a given vulnerability based on applicability, accessibility/exploitability, and impact;
- Establishing the criteria for notifications to the customers and regulatory authorities (as applicable); and
- Triggering the process for updates as required based on the urgency.

Since the risk assessment of a given vulnerability for a certain component requires knowledge of how that component is integrated into the overall software deliverable, it is recommended that the assessment be done by the producers of the software, and communication channels are established to relay the pertinent information to the TC holder and/or operator in a timely manner. AIA recommends the civil aviation industry work together to establish common benchmarks and thresholds for performing risk assessment and a common taxonomy to communicate necessary information across different tiers in the aviation ecosystem.

Additionally, AIA recommends the aviation industry work together to establish a common taxonomy to share information around the impact of vulnerabilities, such as the DHS/CISA developed Vulnerability Exploitability eXchange (VEX) format. VEX provides a mechanism for indicating the impact of a vulnerability on a particular software component.

AIA recommends that regulators require organizations in the aviation ecosystem implement vulnerability management processes for their products, and flow similar requirements to their suppliers. The regulators should establish quantitative expectations for performing analysis of vulnerability and reporting requirements based on exploitability and impact to safety.

2.3.2 Minimum Elements of SBOMs

AIA recommends that SBoMs for aircraft components include information about any third-party procured components such as free and open-source (FOSS) and COTS components. Organizations can choose to include information about custom components, but that should not be an expectation.

Organizations creating SBoMs are encouraged to use industry standard formats like SPDX, CycloneDX and not create proprietary formats. The minimum data fields of an SBoM as defined by NTIA should be incorporated into the SBoM:

- Supplier Name: The name of the entity that creates, defines, and identifies components.
- Component Name: Designation assigned to a unit of software defined by the original supplier.
- Version of the Component: Identifier used by the supplier to specify a change in software from a previously identified version.
- Other Unique Identifiers: Other identifiers that are used to identify a component or serve as a lookup key for relevant databases.
- Dependency Relationship: Characterizing the relationship that an upstream component X is included in software Y.
- Author of SBoM Data: The name of the entity that created the SBoM data for this component.
- Timestamp: Record of the date and time of the SBoM data assembly.

3 Conclusions

In implementing SBoMs, the civil aviation industry must recognize the benefits of understanding the system engineering dependencies on both software and hardware components and protect both aircraft products and ground support across the civil aviation industry.

From an aviation industry perspective, the development of SBoM standards and reporting methods would greatly benefit the industry, specifically in the areas of vulnerability management, code verification, and assisting efforts in read across resulting from specific incidents.

Benefits to be realized from the civil aviation implementation of SBoM include; better understanding of software configurations and dependencies as they impact aircraft and ground support system design, increased awareness of potential system vulnerabilities and ability to conduct corrective and preventative actions and support the rapidly increasing speed and effectiveness of incident response.

To this end, the AIA Civil Aviation Subcommittee recommends a multi-phased plan for how the civil aviation industry will adopt and update its practices to develop and maintain SBoM information specifically for its critical aviation industry products and services.

AIA recommends that the civil aviation industry quickly establishes the following phased approach for generating, consuming, and sharing SBoMs:

- Develop the context for use and minimum expectations for SBoMs.
- Update industry guidance to include SBoMs as a required artifact for software release.
- Encourage adoption of industry standards for the creation of SBoMs,
- Establish infrastructure for storage and use of SBoMs as an input to the Vulnerability Management Process.
- Conduct Proof of Concept and table-top exercises to understand the organizational flow of information during a potential incident. AIA also recommends that the civil aviation industry collaborate on creating processes that would aid organizations in efficiently assessing and responding to vulnerabilities:
- Broader collaboration among industry members around sharing information related to vulnerabilities.
- Establishing Vulnerability Management processes at the organizational level.
- Creating confidential channels for notification of the impact of vulnerabilities on systems to the pertinent stakeholders.

This phased implementation plan should include:

- Phase I - Develop civil aviation industry context for SBoMs (as recommended in this AIA Report).
- Phase II - Define civil aviation Minimum Elements & Dependencies (from AIA WP with civil aviation context).
- Phase III - Establish Prototype civil aviation SBoM Database (w/contributions from partners in SPDX and/or CycloneDX format)
- Phase IV - Conduct Proof of Concept Demonstration with AIA civil aviation Members in Functional Verification Test

To support this plan, AIA also recommends both civil aviation regulations and industry standards be updated to encourage the generation and maintenance of industry defined SBoMs as a part of the software

configuration management processes and require the organizations in the aviation ecosystem to implement vulnerability management processes that use SBoMs to detect and address vulnerabilities in a timely manner.

Since the risk assessment to understand the exploitability and impacts of a given vulnerability in a system may require implementation-level knowledge, it is recommended that the assessment be done by the producers of the software. Communication channels should also be established to relay the pertinent information to the TC holder and/or operator in a timely manner. In the future, we expect the civil aviation industry will work together to establish common benchmarks and thresholds for performing risk assessment and a common taxonomy to communicate the information across different tiers in the aviation ecosystem.

The aviation ecosystem is very complex with software suppliers at varied levels of maturity; hence supply chain processes should be updated to accommodate for the variedly mature suppliers. Organizations should be responsible for assessing the vulnerability management processes within their suppliers, flow the responsibility for timely analysis and notification requirements to the supplier, or incorporate alternate means of compliance in case the supplier does not have a robust vulnerability management process. This may include requiring the delivery of SBoMs, or list of the third-party libraries incorporated in the delivered software or the software code itself, and any other information that would facilitate vulnerability management.

In conclusion, AIA and the civil aviation industry must take advantage of the current focus on SBoMs by updating baseline requirements to establish an aviation industry approach for the generation and maintenance of SBoMs, and enabling the industry to leverage this information with capabilities and tools for a more efficient and timely vulnerability management.

4 Abbreviations

AD	Airworthiness Directive
AIA	Aerospace Industries Association
BOM	Bill of Materials
CAGE	Commercial and Government Entity
CFR	Code of Federal Regulations
COTS	Commercial Off the Shelf
DAH	Design Approval Holder
DOD	Department of Defense
EO	Executive Order
FAA	Federal Aviation Administration
IT	Information Technology
NDIA	National Defense Industrial Association
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Internal Report
NTIA	National Telecommunications and Information Administration
OSS	Open Source Software
OWASP	Open Worldwide Application Security Project
SBoM	Software Bill of Materials
SCI	Software Configuration Index
SPDX	Software Package Data Exchange
SW	Software
TC	Type Certificate

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association
1000 Wilson Boulevard, Suite 1700 | Arlington, VA 22209-3928 | 703.358.1000 | www.aia-aerospace.org

US	United States
VEX	Vulnerability Exploitability eXchange

5 List of References

Reference	Title
14 CFR 21	Certification Procedures for Products and Articles
AC 20-115D	Airborne Software Development Assurance Using EUROCAE ED-12() and RTCA DO-178()
AC 21-43A	Production Under 14 CFR Part 21, Subparts F, G, K, and O
AC 23.1309-1E	System Safety Analysis and Assessment for Part 23 Airplanes
AC 25.1309-1A	System Design and Analysis
AC 27-1B	Certification Normal Category Rotorcraft
AC 29-1B	Certification of Transport Category Rotorcraft
AC 33.28-1	Compliance Criteria for 14 CFR 33.28, Aircraft Engines, Electrical and Electronic Engine Control Systems
AC 33.28-2	Guidance Material for 14 CFR 33.28, Reciprocating Engine, Electrical and Electronic Engine Control Systems
AC 33.28-3	Guidance Material for 14 CFR 33.28, Engine Control Systems
CycloneDX v1.5	https://cyclonedx.org/docs/1.5/json/
EO 14028	Executive Order on Improving the Nation's Cybersecurity
FAA Order 8040.4C	Safety Risk Management Policy
FAA Order 8110.49A	Software Approval Guidelines
FAA Order 8110.4C	Type Certification Process

Reference	Title
NISTIR 8060	Guidelines for the Creation of Interoperable Software Identification (SWID) Tags
NTIA SBoM Minimum Elements	https://www.ntia.doc.gov/files/ntia/publications/SBoM_minimum_elements_report.pdf
RTCA DO-178B	Software Considerations in Airborne Systems and Equipment Certification
RTCA DO-178C	Software Considerations in Airborne Systems and Equipment Certification
RTCA DO-248C	Supporting Information for DO-178C and DO-278A
RTCA DO-330	Software Tool Qualification Considerations
RTCA DO-331	Model-Based Development and Verification Supplement to DO-178C and DO-278A
RTCA DO-332	Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A
RTCA DO-333	Formal Methods Supplement to DO-178C and DO-278A
SAE AS 9115A	Quality Management Systems – Requirements for Aviation, Space, and Defense Organizations for Deliverable Software
SPDX v2.3	https://spdx.github.io/spdx-spec/v2.3/