Cybersecurity Interface Agreement

Revision

Version 5
4/22/24 4:18 PM

Author

Charles Wilson

Abstract

This document details the process to be used to establish the cybersecurity interface agreement between a supplier and the customer organizations.

Group / Owner

Security / Systems Security Analyst

Motivation

This document is motivated by the need to have formal agreements in place for the development of security-related elements by a supplier to be used in products subject to compliance with standards such as **ISO/SAE 21434** and **ISO 26262**.

License

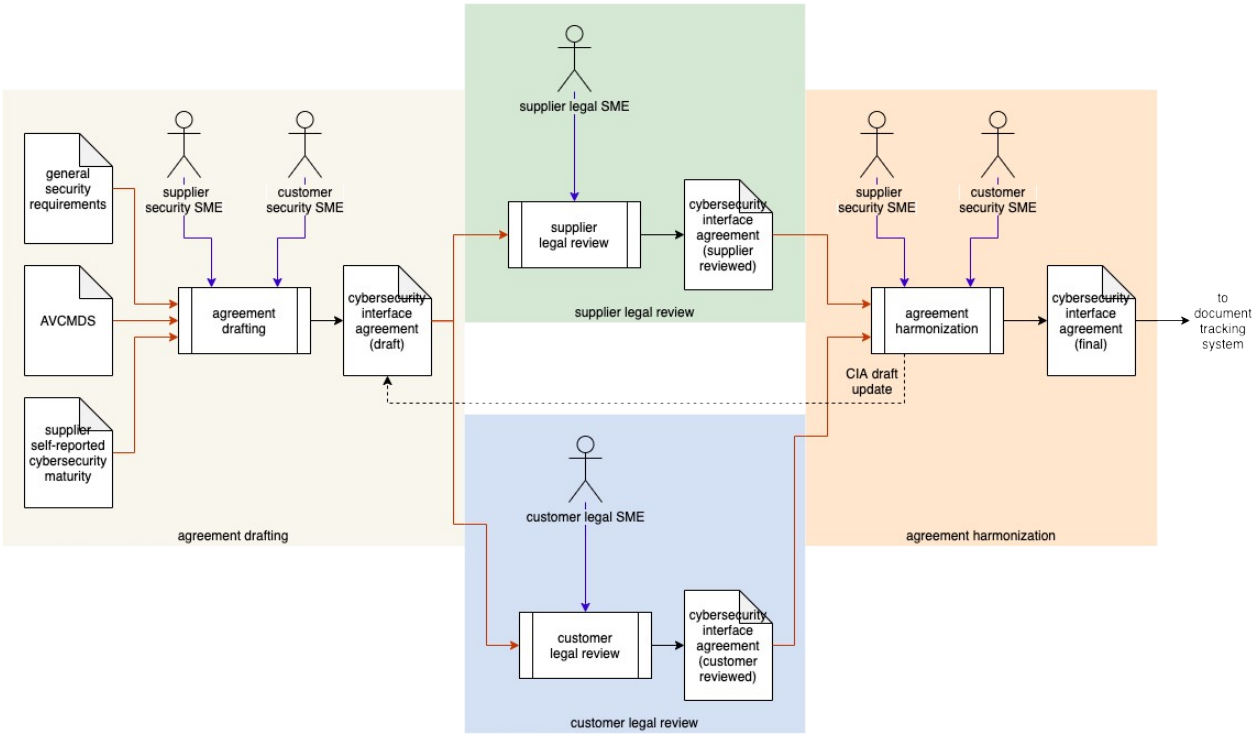
Overview

The **Cybersecurity Interface Agreement** is intended to establish the following:

- identity of responsible individuals
- understanding of supplier capabilities
- responsibility of both consumer and supplier for the various AVCDL work products
- agreement upon the confidentiality level for the various AVCDL work products
- relevant comments of both consumer and supplier

Note: As the **AVCDL Cybersecurity Interface Agreement** is a legal agreement, it is a tracked document.

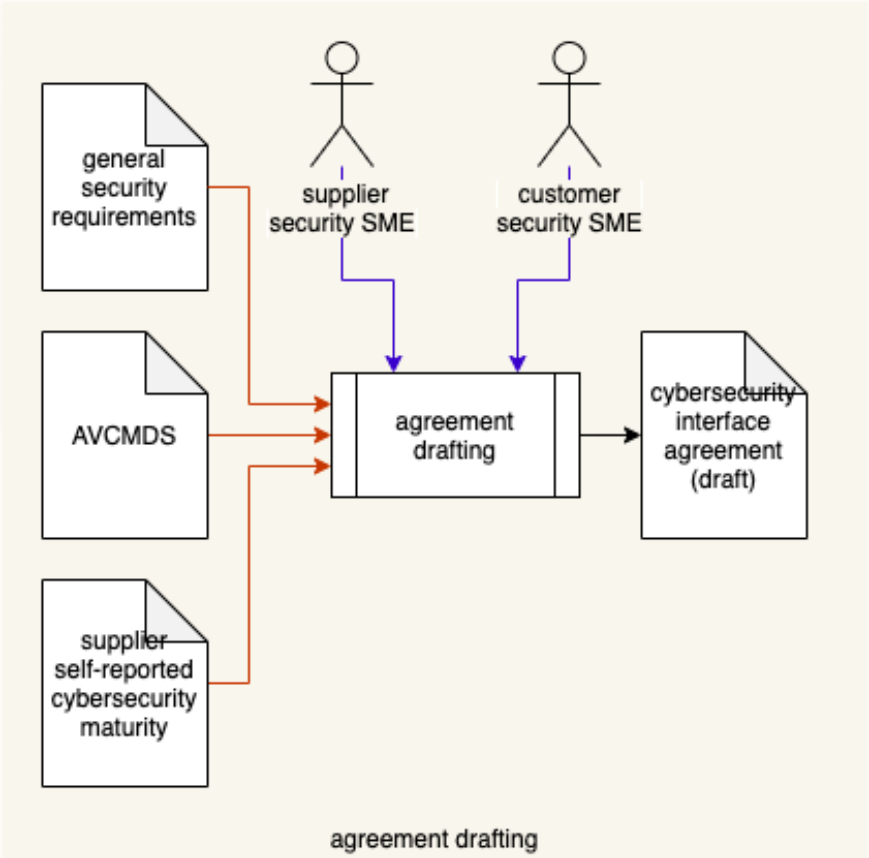
The following diagram illustrates the process to be used:



Process

Agreement Drafting

Inputs	General security requirements AVCMDS Supplier self-reported cybersecurity maturity
Outputs	Cybersecurity Interface Agreement (draft)
Participants	Supplier Security SME Customer Security SME



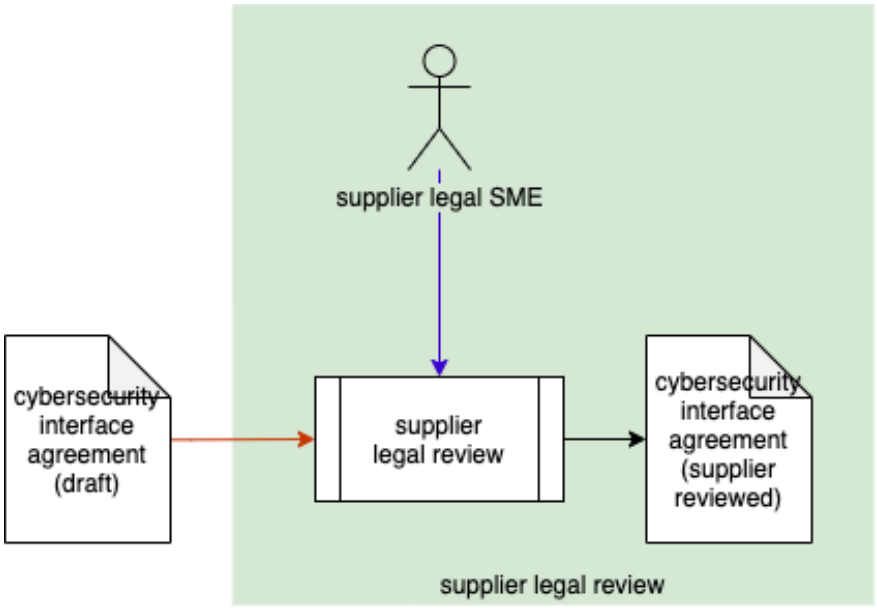
The **general security requirements** (*see note below*) for the element being supplied by the vendor, **AVCMDS (Autonomous Vehicle Cybersecurity Manufacturer Disclosure Statement)** worksheet [12], and **supplier self-reported cybersecurity maturity** report [13] are used by the supplier and customer security SMEs to create a **cybersecurity interface agreement draft**. This should be done using the **AVCDL** [9] as a basis for activities to be undertaken. A template [11] is provided for this purpose.

Note: The **general security requirements** referred to represent a subset created from the **global security catalog** [14] based on the general characteristics of the element under consideration. Tailoring [15] of these requirements will be done after the **cybersecurity interface agreement** is in place and work has begun.

Note: An additional document, **Understanding Cybersecurity Interface Agreements** [10], is provided detailing the use of the interface agreement template.

Supplier Legal Review

Inputs	Cybersecurity Interface Agreement (draft)
Outputs	Cybersecurity Interface Agreement (supplier reviewed)
Participants	Supplier Legal SME

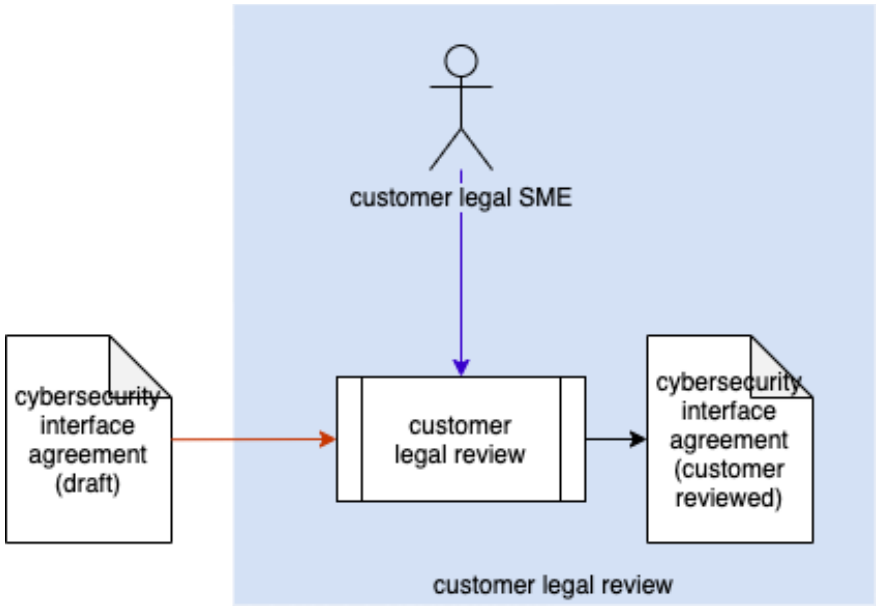


The **cybersecurity interface agreement (draft)** is reviewed by the supplier legal SME. A **cybersecurity interface agreement (supplier reviewed)** is created via annotation.

Note: This activity and the **Customer Legal Review** may be performed in parallel.

Customer Legal Review

Inputs	Cybersecurity Interface Agreement (draft)
Outputs	Cybersecurity Interface Agreement (customer reviewed)
Participants	Customer Legal SME

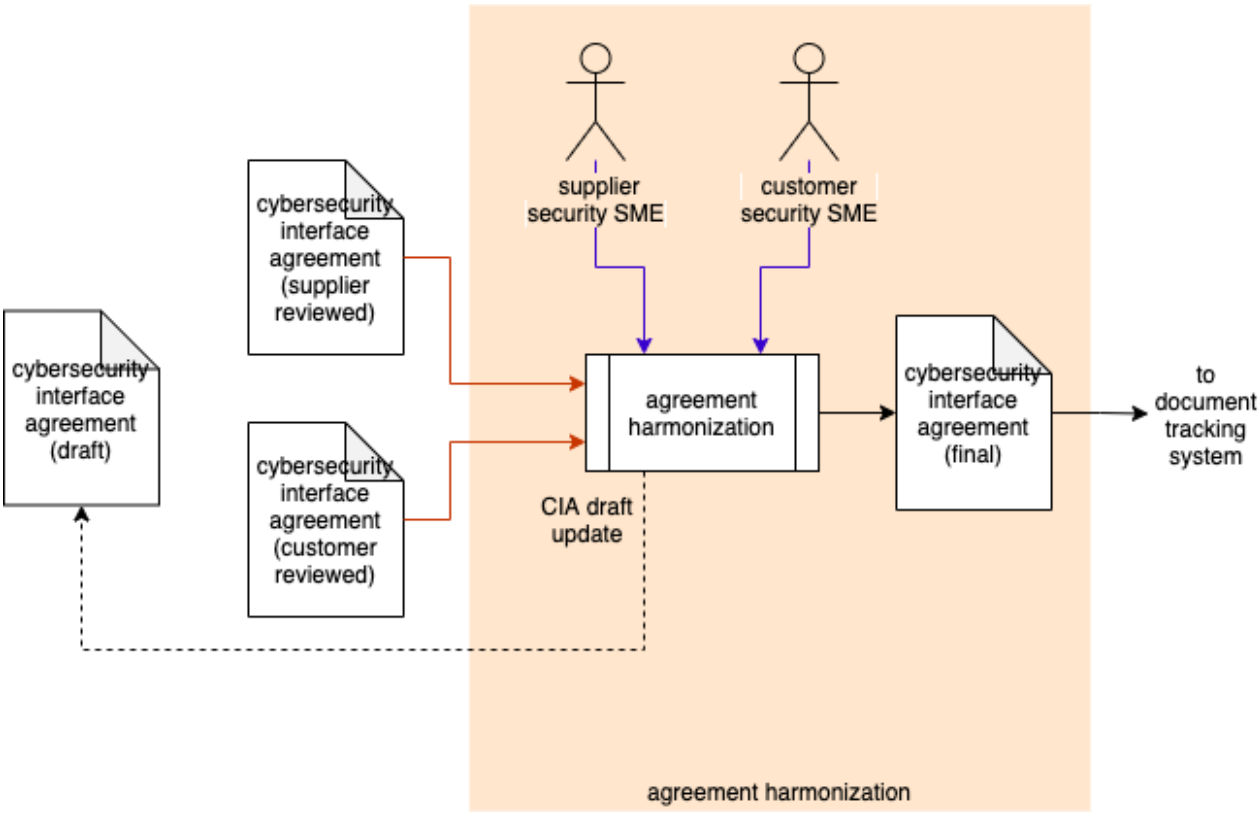


The **cybersecurity interface agreement (draft)** is reviewed by the supplier legal SME. A **cybersecurity interface agreement (customer reviewed)** is created via annotation.

Note: This activity and the **Supplier Legal Review** may be performed in parallel.

Agreement Harmonization

Inputs	Cybersecurity Interface Agreement (supplier reviewed) Cybersecurity Interface Agreement (customer reviewed)
Outputs	Cybersecurity Interface Agreement (final)
Participants	Supplier Security SME Customer Security SME



The **cybersecurity interface agreement (supplier reviewed)** and **cybersecurity interface agreement (customer reviewed)** are used by the supplier and customer security SMEs to harmonize any differences. If there are unresolved issues or questions, the harmonized information is fed back into the **cybersecurity interface agreement (draft)** triggering another round of reviews. If there are no unresolved issues or questions, the harmonized information is integrated to **create the cybersecurity interface agreement (final)**. This document is the transferred to the document tracking system for management sign-off and archiving.

References

1. **UNECE trans WP.29 GRVA 2019 2 - World Forum for Harmonization of Vehicle Regulations: Proposal for a Recommendation on Cyber Security**
   https://unece.org/fileadmin/DAM/trans/doc/2019/wp29grva/ECE-TRANS-WP29-GRVA-2019-02e.pdf
2. **Software Package Data Exchange® (SPDX®)**
   https://spdx.dev/wp-content/uploads/sites/41/2017/12/spdxversion2.1.pdf
3. **ISO 19770-2:2015 Information technology - IT asset management - Part 2: Software identification tag**
   https://www.iso.org/standard/65666.html
4. **NIST IR 8060 Guidelines for the Creation of Interoperable Software Identification (SWID) Tags**
   https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8060.pdf
5. **NIST SP 800-181 NICE Cybersecurity Workforce Framework (NCWF)**
   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf
6. **Responsibility Assignment Matrix**
   https://en.wikipedia.org/wiki/Responsibility_assignment_matrix
7. **Capability Maturity Model**
   https://en.wikipedia.org/wiki/Capability_Maturity_Model
8. **Software Bill of Materials**
   https://www.ntia.gov/sbom
9. **AVCDL** (primary document)
10. **Understanding Cybersecurity Interface Agreements (AVCDL secondary document)**
11. **AVCDL Cybersecurity Interface Agreement template.xlsx (AVCDL template document)**
12. **AVCMDS Worksheet template.xlsx (AVCDL template document)**
13. **AVCDL vendor CMM template.xlsx (AVCDL template document)**
14. **Global Security Requirements (AVCDL secondary document)**
15. **Product-level Security Requirements (AVCDL secondary document)**