# Title

I'm Charles Wilson, senior principal engineer at motional responsible for cybersecurity development lifecycle practice.

This presentation will cover the autonomous vehicle cybersecurity manufacturers disclosure statement (or AVCMDS).

# Supply Chain Training Path

This diagram shows the overall AVCDL supply chain training path.

If you’re taking this training, it’s assumed that you’ve already completed the supply chain overview training.

This training covers the manufacturer disclosure statements or AVCMDS.

Additional trainings will cover

* supplier cybersecurity maturity,
* vendor cybersecurity process to AVCDL mapping,
* cybersecurity requirements,
* tailoring the cybersecurity interface agreement,
* service level agreements (SLAs),
* software bill of materials (SBOM),
* attack surface analysis,
* and threat modeling.

# Introduction

Here’s an image of sailors taking part in a Battleship tournament on a battleship. Just imagine if you were playing, knew all the rules, but weren’t allowed to see where your ships were. That’s the situation we’re in without the AVCMDS.

When we consider the title of this training, **autonomous vehicle cybersecurity manufacturer disclosure statement**, two things come to mind.

One, what is a manufacturer disclosure statement?

And two, what does it have to do with cybersecurity?

The answer to the first question is straightforward. A manufacturer disclosure statement is a description of the materials, sources, storage, and application procedures for a product from a manufacturer.

The use of manufacturer disclosure statements goes back thousands of years.

The second is more difficult question. What does a manufacturer disclosure statement have to do with cybersecurity?

For that we have to look at how we treat suppliers in an automotive context with respect to cybersecurity in general.

Until very recently the responsibility for cybersecurity has fallen upon the OEMs directly.

Suppliers would provide a functional device, component, or piece of software.

That would be integrated up through the various tiers and when it reached the OEM, they would be responsible for any cybersecurity controls necessary in order to satisfy their cybersecurity requirements.

This works until it doesn’t.

UNECE R155, which is in force in all of Europe and various countries throughout the world, requires that cybersecurity exist not only as a responsibility of the OEM, but also throughout the supply chain.

This recognizes the complexity of today’s computer-based systems within vehicles.

Because there was no requirement for cybersecurity controls at the vendor level there was no need to have a way to determine what controls were being put in place within the supplier’s organization.

Without information that tells us that a supplier is doing certain things in the cybersecurity context, we have to assume that they are doing nothing.

Because of that, we're limited in terms of the types of analysis that we can perform on components provided by suppliers to ensure that cybersecurity controls are in place.

One tool we have is the attack surface analysis. But the information provided by an attack surface analysis are limited.

We could also do penetration testing, but we run into the same type of problem.

We're doing an analysis on something after the fact.

We're not looking at what controls were put in place by default, and what good behaviors are being used by the company.

A more fundamental problem is that even though we have attack surface analysis and penetration testing at our disposal, these are happening at the wrong point in time.

We've already selected the vendor and we've already received the complement in some cases.

What we'd like to be able to do is incorporate an instrument at the RFI stage of supplier selection so we’re able to weigh the cybersecurity controls that one vendor has over another.

This allows us to estimate the amount of work that we're going to have to put in if it's determined that the functionality that a particular vendor provides outweighs the other vendor selection factors.

The AVCMDS Is a manufacturer disclosure statement that's specifically tailored to provide the kinds of information that we will need to know in order to make determinations of this very sort.

It's based on an existing model that's used within the medical industry known as the MDS2 (the manufacturer disclosure statement for medical device security).

Much of the information is in common with that particular instrument.

The AVCMDS is not intended to be a be all and end all, but is a survey of the capabilities enabling apples to apples comparisons between vendors.

We use it to determine the resources that are going to be necessary to ensure that we have the level of cybersecurity needed to maintain the safe operation of the vehicle.

# AVCMDS Use in Supplier Selection

Here we can see how various documents key to supply chain cybersecurity relate and where in the supplier selection process they live.

We can see that the AVCMDS is a precursor to the creation of the tailored cybersecurity requirements and is necessary in the request for information or RFI stage.

# AVCMDS Material

There are three documents within the AVCDL document set that support the creation of the AVCMDS.

These are

* the **Autonomous Vehicle Cybersecurity Manufacturers Disclosure Statement** secondary document
* the blog post **AVCMDS Autonomous Vehicle Cybersecurity Manufacturers Disclosure Statement**
* and the **Manufacturers Disclosure Statement for Autonomous Vehicle Cybersecurity AVCMDS** template.

# AVCMDS Documentation

Here you can see the relationship between the various AVCDL documents covering the AVCMDS.

We can see that the **AVCMDS worksheet template** is used to create the **supplier cybersecurity disclosure statement**. A specific instance of the AVCMDS template.

The dotted lines surrounding those two documents Is used to indicate that both the **autonomous vehicle cybersecurity manufacturers disclosure statement** secondary document and the **AVCMDS autonomous vehicle cyber security manufacturer disclosure statement** blog posts refer to both of those documents taken together.

AVCMDS Workflow

Here's the workflow used to create the suppliers AVCMDS.

This diagram is taken from the AVCMDS secondary document.

As you can see, there are two activities that take place, the practices assessment and the worksheet review.

In the practices assessment activity, the supplier’s cybersecurity SME uses the supplier’s cybersecurity practices to complete the AVCMDS Worksheet template.

This results in the creation of an AVCMDS worksheet draft specific to the supplier.

This draft is then reviewed by the customer’s cybersecurity SME.

Any deficiencies found are fed back to the supplier to create an update of the draft.

Once it's been determined that there are no deficiencies the worksheet is considered to be final and is entered into the customer's document tracking system.

AVCMDS Worksheet Details

Now let's go over some general information that you'll need in order to fill out the AVCMDS worksheet.

Base Information

The first section of the worksheet to be completed is the base information.

This section is labeled documentation or DOC.

It contains seven items.

* The manufacturer's name
* The device description
* The device model
* The document ID
* The manufacturer contact information
* The intended use of the device in a network connected environment
* And the document release date

It's important to note here that the AVCMDS is relevant to a specific device or product being provided by the supplier to the customer.

This is why we see reference to a specific device description and model, as well as, the corresponding document ID and release date.

Summary Information

The base information is used to populate the summary at the top of the worksheet.

As you can see here all of the fields in yellow are transferred automatically to the fields in green.

These fields should not be modified as they are auto-filled.

Worksheet Topics

The AVCMDS worksheet covers 24 topics.

They're listed here.

Rather than read them off, I’ll leave them on the screen for a bit and give you some time to look them over.

Worksheet Columns

Each question is provided on its own line, and each line has five columns associated with it.

The fields include

* the ID, which is unique to the question and the section
* the question itself
* the answer
* a note
* And an explanation, should one be necessary

Answer Options

Aside from the base information whose answers are in the form of text strings, all of the other questions are answered via drop-downs.

As you can see here, we have the options of

* Yes
* No
* not applicable
* and see notes

Default Answer Values

A default answer has been provided for each of the questions.

The hope is that these will represent a typical state of affairs, and that any deviations should be noteworthy.

Answer Notes

When an answer requires a qualification, a note should be used.

As seen here, this particular question references note 6.

The answer is yes, but it's a qualified yes.

Answer Explanations

In the rare case when a note will not suffice to add clarity to an answer, the explanation field should be used.

The explanation should be long form text providing enough background so that the customer can evaluate the supplier’s rationale.

As-Is Assessment

An important note.

The AVCMDS is an “as-is” assessment.

It’s about what the supplier is doing today.

Any question where the supplier reports that they have a process or do an activity should be verifiable.

Suppliers should be informed that their answers are subject to requests for evidence.

AVCDL on GitHub

All AVCDL materials, both in source and distribution forms, are available on our GitHub site, as shown here.

Because of the size of the repository, it's recommended that you either clone the repository or download a zip archive of it if you're not familiar with using Git.

Instructions for downloading a ZIP archive are linked to on the repository’s front page.

Supply Chain Training Path – Next Steps

The next step in this training sequence is to complete the two other courses at this level, if you haven’t already.

The supplier maturity training, covers how a supplier self-reports the maturity of their processes in the context of the AVCDL.

The vendor process mapping training covers how to take established vendor processes and map them to the corresponding AVCDL processes.

This helps to ensure that no gaps will exist between the vendor and the customer in the area of cybersecurity.

Once the three trainings at this level are complete, you should proceed to the security requirements training.

References

Here are references to the source material used in the creation of this presentation.

They'll also be included in the video description.

Additionally, this presentation’s source material will be provided on the AVCDL GitHub repository.

The image of sailors playing Battleship is a publicly available image from the US government.