Ford Supplier Cyber Assurance Statement of Work (FSCA-SOW)

Version 4

FORD CONFIDENTIAL

Revision History

Date	Version	Notes
29-Jun-20	1.7	Removed Checklist and added it as an external attachment, UNECE Checklist added, AV sensor requirements added, ISO SAE compliance added.
18-Dec-20	1.8	Removed Spec/Req. links from reference table, Security ARL callouts Changed flowchart, added a new column non-cyber relevant, section 3 task changed deliverable titles, GPDS Timing deliverables table, added 'type' to table 3, Moved Post Job One (J1) Support section to section 4. New Table 3 category 'type', VDOC073888 under CMA section, Physical security req. supporting content, New Section Module Cybersecurity Relevance Assessment, New Section Module Cybersecurity Derivative Analysis, New Section Module V&V Report, New Section Final Cybersecurity Assessment, New Section Published Vulnerabilities Resolution, Table 6 Key Management Req. under section Cryptographic Key Management
29-Jun-21	1.9	New - link – UNECE R155, New - Legal statement in Introduction, New - Service Desk link in Scope, New- Section P2P, New – Section Secure Boot, New - CAN Network Gateway Re. section, New - Advanced Operating System Req. section, New - In-Vehicle Ethernet Req. section, New - Ethernet Protocol Req. section, New -Driver Assistance and Autonomous Vehicle Req. section, New -Digital Key section, New - Security Logging Req. section, Moved - Cryptographic Key Management Req section, New – Embedded Manifest signing req. section, New - Section FNV4 Architecture Module Security Req. New - ISO/SAE 21434 reference throughout document, New - Section 4.12 Cryptographic Export Documentation. Removed - SAE J3061, Removed - Cybersecurity Threat Template - Cybersecurity Threat UNECE Compliance Checklist, Removed - Vehicle Key Back-End Authentication – Cybersecurity, from core requirements table.
7-Dec-21	2	New- Cybersecurity Interface Agreement New- Section 3.2.2.1 SyncP New – Section 4.16 Cybersecurity Triage Support New – Section 4.17 Cybersecurity Monitoring New – Section Support of Architecture/Vehicle Threat Model
31-March-22	3	New – Section Vehicle Security Channel PARSED Spec Section 3.2.2.15 – added Vehicle Key Back-End Authentication req to digital key Section 3.2.2.18 – added RQT-001403-724736 Section 3.2.2.21 – added note that suppliers shall use service $29 instead of service $27 if able Section 3.2.2.21 – added the following FNV4 requirements RQT-001403-724723, RQT-001403-724524, RQT-001403-724585, RQT-001403-724784, RQT-001403-724738, RQT-001403-724744, RQT-001403-724783, RQT-001403-724727, RQT-001403-724666
June-22	4	Added Software Bill of Materials (SBOM) section Retired Derivative Analysis, Item Definition, and Risk and Remediation Template

TABLE OF CONTENTS

1 INTRODUCTION 5

1.1 SCOPE 5

1.2 FSCA-SOW APPLICABILITY 5

1.3 SUPPLIER DELIVERABLES AND TIMING 5

1.4 DOCUMENTATION AND REFERENCES 6

2 FORD CYBER ASSURANCE HIGH LEVEL PROCESS 7

3 TASK DEFINITION 8

3.1 MODULE CYBERSECURITY RELEVANCE ASSESSMENT 8

3.1.1 Inputs 8

3.1.2 Process 8

3.1.3 Outputs 8

3.2 CONTRACT AWARD 8

3.2.1 Inputs 8

3.2.2 Process 8

3.2.3 Outputs 17

3.3 KICKOFF 18

3.3.1 Inputs 18

3.3.2 Process 18

3.3.3 Outputs 19

3.4 MODULE CYBER SECURITY PLAN 19

3.4.1 Process 19

3.4.2 Outputs 19

3.5 MODULE THREAT ANALYSIS & RISK ASSESSMENT (TARA) 20

3.5.1 Inputs 20

3.5.2 Process 20

3.5.3 Outputs 22

3.6 MODULE CYBERSECURITY REQUIREMENTS 22

3.6.1 Inputs 22

3.6.2 Process 22

3.6.3 Outputs 22

3.7 MODULE VERIFICATION AND VALIDATION(V&V) PLAN 23

3.7.1 Inputs 23

3.7.2 Process 23

3.7.3 Outputs 25

3.8 INITIAL CYBERSECURITY ASSESSMENT REVIEW 25

3.8.1 Inputs 25

3.8.2 Process 26

3.8.3 Outputs 26

3.9 MODULE VERIFICATION AND VALIDATION (V&V) REPORT 26
Inputs *26*
3.9.1 Process *26*
3.9.2 Outputs *26*
3.10 PENETRATION TESTING 26
3.10.1 Inputs *26*
3.10.2 Process *27*
3.10.3 Outputs *27*
3.11 FINAL CYBERSECURITY ASSESSMENT REVIEW 27
3.11.1 Inputs *27*
3.11.2 Process *28*
3.11.3 Outputs *28*
4 GENERAL CYBERSECURITY REQUIREMENTS 29
4.1 ROAD VEHICLES — CYBERSECURITY ENGINEERING 29
4.2 THIRD-PARTY TESTING 29
4.3 DOCUMENTATION 29
4.4 SUPPLIER DELIVERABLES 29
4.5 PRODUCTION-READY SECURITY STATE 30
4.6 INFORMATION SHARING/VULNERABILITY, EXPLOIT, AND INCIDENT DISCLOSURE 30
4.7 PUBLISHED VULNERABILITIES RESOLUTION 30
4.8 FORD INCIDENT RESPONSE TRIAGE PROCESS 30
4.9 SUB-SUPPLIER(S) 31
4.10 SECURE CODING PRACTICES 31
4.11 CRYPTOGRAPHIC EXPORT DOCUMENTATION 31
4.12 PROTECTION OF CRYPTOGRAPHIC KEYS 31
4.13 CONNECTED VEHICLE TECHNOLOGY 31
4.14 CYBER ASSURANCE REVIEWS 32
4.15 OPEN-SOURCE SOFTWARE 32
4.16 SOFTWARE BILL OF MATERIALS (SBOM) 32
4.17 CYBERSECURITY TRIAGE SUPPORT 33
4.18 CYBERSECURITY MONITORING 33
4.19 SUPPORT OF ARCHITECTURE/VEHICLE THREAT MODEL 33
APPENDIX A. CONTACT DETAILS 34
APPENDIX B. CYBERSECURITY INTERFACE AGREEMENT 35
APPENDIX C. TERMINOLOGY AND ABBREVIATION 36

1 Introduction

The Ford Supplier Cyber Assurance Statement of Work (FSCA-SOW) defines the Cybersecurity related activities required of a Supplier of products or services, Supplier to Ford and supplements the contract between Ford and Supplier for such supply of products or services ("Agreement"). Ford and Supplier are as defined in the Agreement. In the event of conflict between the terms in this FSCA-SOW and those in the Agreement, the terms in the Agreement shall prevail. All references to "Ford" in this FSCA-SOW shall mean Buyer as defined in the Agreement.

Reminder: the contents of this FSCA-SOW is Ford Confidential Information and Ford copyrighted material and must be treated as such according to the terms of the Agreement, including non-disclosure, limitations on use, and limitations on copying.

This FSCA-SOW supplements the Ford Motor Company Production Purchasing Global Terms and Condition ("PPGTCs") which are referenced in the Purchase Order. Any conflicts between this FSCA-SOW and the PPGTCs shall be governed by the PPGTCs, unless specifically agreed in writing by an authorized Ford Motor Company representative (e.g., Purchasing buyer).

1.1 Scope

This document defines the requirements and deliverables to be executed by Supplier as part of a secure design process for the products or services to be provided to Ford.

In general, the activities consist of:

- Cybersecurity capabilities and posture of the Supplier
- Cybersecurity Requirements
- Methodical approach of identifying and assessing cyber threats and selecting countermeasures
- Supplier Security Design Reviews
- ISO/SAE 21434 Requirements

Any ECU Supplier questions regarding this FSCA-SOW can be submitted to the Product Development Software Sourcing Service Desk by the assigned Ford Design & Release (D&R) Engineer. Suppliers should submit questions via their product team/engineer. Suppliers do not have access to Service Desk.

1.2 FSCA-SOW Applicability

The Ford Supplier Cyber Assurance Statement of Work applies to all Cybersecurity relevant electronic systems that involve Tech Products or firmware. The FSCA-SOW shall apply to Goods, Services, or Tech Products that involves any of the following:

- Is connected physically or wirelessly to any internal vehicle communication network
- Are indirectly connected to any vehicle communication network
- Include data acquisition systems or management system(s) comprising collections of sensors and communication links that sample, collect, and/or provide data for display, storage, or further processing
- Physical security of the vehicle
- Ford will perform a Cybersecurity Relevancy Assessment at the start of the program to confirm the work path required as per section 2. See the lead Ford engineer for your component for confirmation of this Cybersecurity Relevancy Assessment.

1.3 Supplier Deliverables and Timing

Supplier deliverables required in this FSCA-SOW shall be provided in line with agreed timing relative to Ford Global Product Development System milestones. The Supplier shall coordinate cyber assurance deliveries with their Ford point of contact or the appropriate Ford personnel (e.g., Design and Release (D&R) and Ford Cybersecurity Application/Engagement Engineers), as designated by Ford.

If the Ford program is identified for I-Build, the ECU Supplier shall be required to deliver developmental software, containing base technologies, iteratively between PS and UPV2. Ford will need to review and approve of the content plan for these 4 increments, each of which shall be delivered at an interval of 4-6 weeks.

1.4 Documentation and References

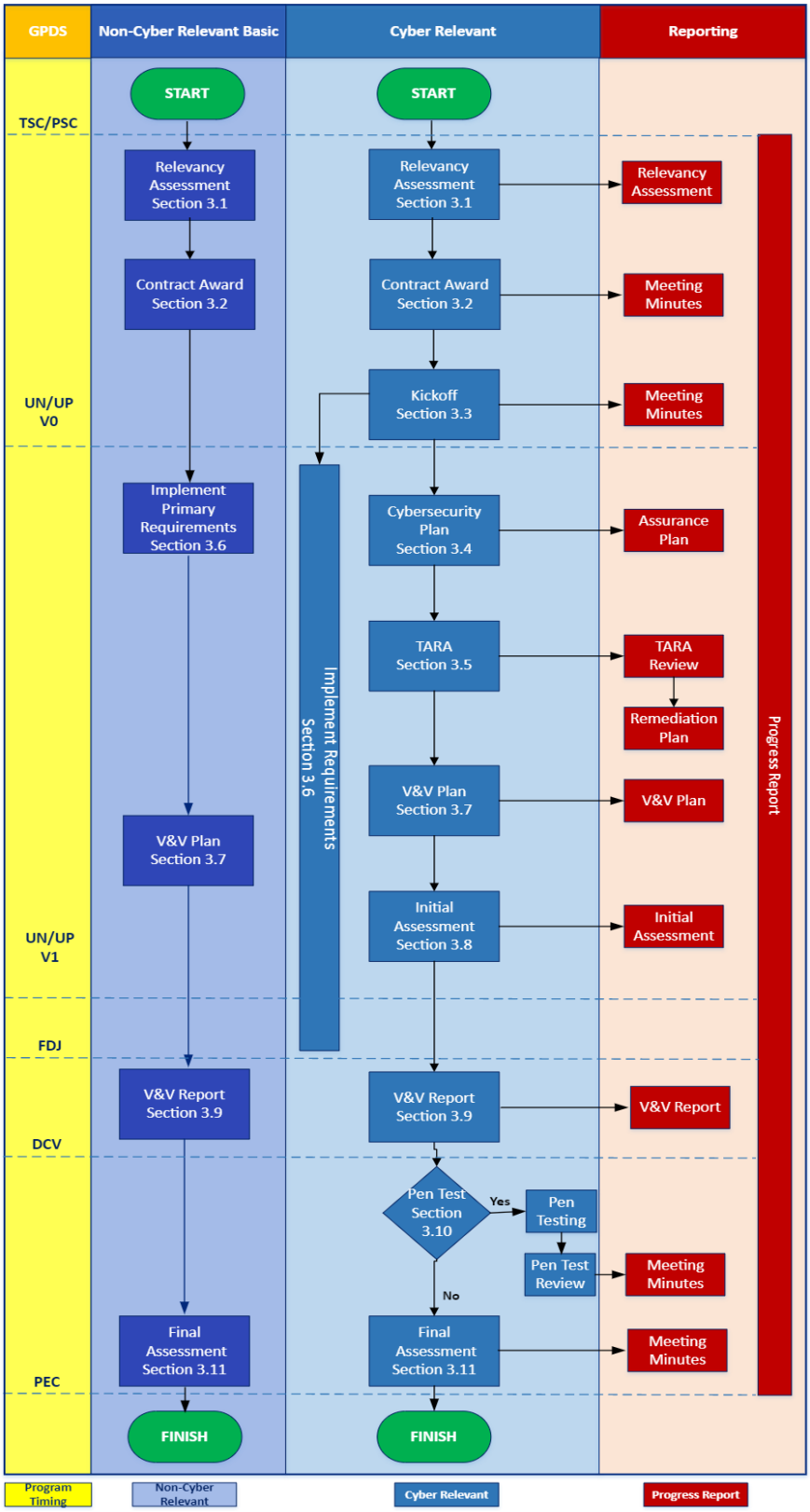
The Supplier shall use the most current version available of the documents listed in Table 1. Suppliers should obtain the needed documents from their product team/engineer. In the event that Ford, or an industry standard, changes which would result in a change to Supplier's Goods, Tech Product, Service, or deliverable, Supplier must issue a DCR to which Ford and Supplier will review the implications. Supplier may obtain documents from Ford.

Table 1 References

Reference	Document Title
Ford Cyber Assurance Toolbox	The Ford Cyber Assurance Toolbox (FSCA-SOW Toolbox)
UNECE ECE/TRANS/WP.29/2020/79	UN Regulation No. 155
ISO/SAE 21434	Road Vehicles — Cybersecurity Engineering

2 Ford Cyber Assurance High Level Process

The Ford Cyber assurance process to be incorporated into the Supplier product development lifecycle is illustrated below. Details about each process element may be found in the task's definition



3 Task Definition

The Supplier agrees to complete the tasks and provide the deliverables described below.

3.1 Module Cybersecurity Relevance Assessment

Ford uses a set of criteria based on ISO/SAE 21434 to determine the applicability of a given module to the Cybersecurity System of the vehicle type, in line with UNECE R155. These criteria are to be evaluated by the Ford D&R and will fall into one of the three categories as defined below:

A. Cyber Relevant – Shall meet all conditions and deliverables as defined within this document.
B. Non-Cyber Relevant / Quality Management (e.g., modules on private LIN bus / hardwired) - Need to meet the vulnerability disclosure and warranty reporting portion (Section 4) of the of this document. No additional Cybersecurity requirements, deliverables, penetration testing and/or TARA are required.
C. Non-Cyber Relevant - Basic / Corporate Direction (e.g., module on CAN without direct influence on vehicle Cybersecurity) – Must meet the Cybersecurity primary requirements as defined in the Ford Engineering Design Environment (FEDE). Evidence of successful implementation via presentation of test results to the Cybersecurity team shall be provided along with the vulnerability disclosure and warranty reporting portions as found in (Section 4) of this document. No additional Cybersecurity requirements, penetration testing, and/or TARA are required. Follow sections 3.1, 3.2, 3.6, 3.7, 3.9 and 3.11 for all non-cyber relevant deliverables.

3.1.1 Inputs

Ford internal part of onboarding process.

3.1.2 Process

Ford will provide the Cybersecurity Relevant category.

3.1.3 Outputs

The deliverables to be completed depend on the category assignment. Refer to Table 3 for categorization. Section 4 of this document applies to all categories.

Ford shall provide the following as a result of completing this task:

- Cybersecurity Relevant category
- Cybersecurity Preliminary Risk Assessment that will determine secure boot application strategy

3.2 Contract Award

The following shall be initiated at the commencement of the Agreement.

3.2.1 Inputs

The following artifact are required inputs to this task:

- The Agreement

3.2.2 Process

The Supplier shall complete the following at the commencement of the Agreement.

3.2.2.1 Cybersecurity Interface Agreement

The Cybersecurity Interface Agreement is a matrix that defines the owning, supporting, informing, and consulting responsibilities of tasks. The Cybersecurity Interface Agreement is included in this document under Appendix B Cybersecurity Interface Agreement

3.2.2.2 FSCA-SOW Deliverable Timing

The Supplier shall be responsible for completing and submitting the following deliverables per GPDS milestones as provided in Table 2.

Table 2 GPDS Timing Deliverables

Tasks	Complete	Responsible
Module Cybersecurity Relevancy Assessment	UN/UP V0	Ford
Contract Award	UN/UP V0	Ford
Kickoff	UN/UP V0	Ford/Supplier
Module Cybersecurity Plan	UN/UP V1	Supplier
Module TARA Review	UN/UP V1	Supplier
Module Validation and Verification Plan	UN/UP V1	Supplier
Initial Cybersecurity Assessment	UN/UP V1	Ford
Module Cybersecurity Requirements Implemented	FDJ	Supplier
Module Validation and Verification Report	DCV	Supplier
Penetration Testing (if required)	PEC	Supplier
Final Cybersecurity Assessment	PEC	Ford

3.2.2.3 Identification of Supplier Security Lead

The Supplier shall identify and nominate a Security Lead who will be responsible for overseeing and coordinating security efforts for the duration of the product or service's lifecycle. The Security Lead is the security liaison between Ford and Supplier. The Lead's qualification and competencies shall be verifiable, documented, and reviewable by Ford. This person shall be empowered by Supplier to request resources to support the Cyber Assurance design process at all lifecycle phases of the product or service.

3.2.2.3.1 Minimum Security Lead Credentials

Ford recommends that the Cybersecurity Lead should have, at a minimum, the following requirements:

- Progressive experience in the Cybersecurity field
- Strong project management skills, good communication skills, and change management skills

Required duties of the Cybersecurity lead:

- Ensures products and/or services provided to Ford are following relevant Cybersecurity regulations and standards.
- Coordinates and communicates within the Supplier(s) organization, the Supplier responsibilities are related to this FSCA–SOW.
- Ensures that Supplier responsibilities as related to this FSCA-SOW are understood within Supplier organization which includes but is not limited to, training and the reviewing of tasks, metrics, and deliverables.

Cybersecurity certification, such as CISSP, CISM, CISA is strongly recommended.

3.2.2.3.2 Contact Information

The Supplier Security Lead shall be explicitly identified, and contact information shared with Ford, including name, email address, title.

3.2.2.4 The Cyber Assurance Status Reporting

The Supplier shall send a Cyber Assurance remediation status report on a regular basis, to be agreed during project initiation and at key Ford GPDS milestones during the project. This is to identify that the Cyber Assurance work is progressing and that open issues can be resolved in a timely manner.

The Cyber Assurance status report shall include:

- Status of the Cyber Assurance activities in relation to the Cyber Security Plan
- Cyber Assurance activities accomplished during the since last status report
- Cyber Assurance activities planned during the reporting period
- New/open issues related to Cyber Assurance
- Action Item Status
- Discovered vulnerabilities since last reports

3.2.2.5 Compliance with General Cybersecurity Requirements

Refer to the General Cybersecurity Requirements defined in Section 4 of this document.

3.2.2.6 Compliance with In-Vehicle Cybersecurity Requirements

The Supplier shall complete the In-Vehicle Cybersecurity Requirements as defined in Table 3.

The list of In-Vehicle Cybersecurity Requirements released in FEDE at the time of release of this FSCA-SOW revision is included in Table 3. It is the responsibility of the D&R/Program team to ensure that the latest versions of the documents listed in this section are used. Suppliers should obtain the requirements via their D&R or program team contact. Suppliers do not have access the toolbox. Instructions on obtaining the latest version of the Security Requirements is included on the FSCA-SOW Toolbox.

Table 3 Base Cybersecurity Requirements

Req. Number	Title	Type
RQT-001403-706883	Identification and Protection of Security Critical Functions and Data - Cybersecurity	Secondary
RQT-001403-020627	Cybersecurity eSOW Compliance - Cybersecurity	Primary
RQT-001403-020628	Security Algorithms Review	Secondary
RQT-001403-020629	Protection of Security Critical Data accessed via DIDs -Cybersecurity	Secondary
RQT-001403-020655	Protection of Security Function Input & Controls through diagnostic routine 31	Secondary
RQT-001403-020656	Protection of Security Functions Inputs through Hex 2F - Cybersecurity	Secondary
RQT-001403-020657	Message Control on Gateway Modules - Cybersecurity	Secondary
RQT-001403-020661	Memory Read/Write by address of secure critical data - Cybersecurity	Secondary
RQT-001403-020665	Security Critical Data handling in RAM - Cybersecurity	Primary
RQT-001403-020666	Random Number Generators	Secondary
RQT-001403-020667	Access control of micro debug interfaces	Primary
RQT-001403-020668	Elimination of HW & SW backdoor Access - Cybersecurity	Secondary
RQT-001403-020669	Access definition within ECU - Cybersecurity	Secondary
RQT-001403-020671	Secure Default State after Module Reset	Primary
RQT-001403-020672	Software Signing Specification	Primary
RQT-001403-705880	Non-use of Disclosed Secret Key Material - Cybersecurity	Secondary
RQT-001403-704890	FESN Memory Storage	Secondary

Note: RQT-001403-706883 Identification and Protection of Security Critical Functions and Data – Cybersecurity will supersede RQT-001403-020617 and/or RQT-001403-020626. During this transition, Ford will accept compliance/evidence with RQT-001403-020617 and RQT-001403-020626 in lieu of RQT-001403-706883. However, RQT-001403-706883 and associated templates is strongly encouraged. Suppliers will need to produce evidence that critical data and functions identified as part of this process are protected per the agreed template. The procedures and templates are available on the FSCA-SOW Toolbox.

3.2.2.7 CAN Message Authentication Requirements

CAN Message Authentication (CMA) is part of Ford Cybersecurity strategy. For CMA, the Change Management Committee (CCMC) owns and maintains the list of ECUs that are required to meet the CMA requirements on a vehicle program by program basis. Please refer to VDOC086511-Architecture Specific CMA Module List for the most up-to-date list of modules required to support CMA. This list is Ford internal, and the D&R can confirm the applicability of these requirements.

The requirements and specifications for CMA at the time of this version of the FSCA-SOW are listed in Table 4. Suppliers shall obtain the latest versions of these requirements from their D&R or program contact.

Table 4 CMA Requirements

Req. Number	Title
RQT-001403-023402	CAN Message Authentication Pre-Requisites
RQT-001403-023403	CAN Message Authentication Gateway Module Requirements
RQT-001403-023404	CAN Message Authentication ECU Requirements
RQT-001403-701612	Gateway Module Authentication Authenticated Message Routing Policies
VDOC074165	CAN Message Authentication ECG Specifications

Suppliers shall implement CMA requirements ONLY if one of the following conditions are met: (1) the ECU is on this list or (2) the ECU D&R has reviewed its need for CMA and receives approval from the CCMC. Prior to the CCMC review of the module, the module team must complete the Signal Rating assessment, per VDOC073888, as this supports the decision whether to implement the CMA solution.

It is the responsibility of the D&R/Program team contact to ensure that the latest versions of the documents listed in Table 4 are used. Suppliers are recommended to follow Ford issued CMA integration guide for software integration and implementation. Suppliers shall perform Ford issued CMA conformance test for each production software release. For specific questions, please contact Ford CAN Message Authentication Contact with subject line being "CMA Support Needed For [name of ECU] from [name of supplier]".

3.2.2.8 Vehicle Security PARSED Spec

The Vehicle Security PARSED Requirements Specification attachment to the FSCA-SOW describes essential requirements for capturing and reporting security event data associated with the ECU/software for use in production intent vehicles.

Table 5 PARSED Requirement

Req. Number	Title
VDOC124471	Vehicle Security Channel PARSED Spec

3.2.2.9 Point-to-Point Authentication Protocol Requirement

Point-to-Point Authentication Protocol is intended as a security alternative when network topology or other restrictions prevent the use of CAN Message Authentication. ECU's that cannot meet CMA, or do not have an SHE, HSM. Modules required to support Point-to-Point shall implement the requirements identified in Table 6.

Table 6 P2P Requirement

Req. Number	Title
RQT-001403-720105	Point-to-Point Authentication Protocol Requirement – Cyber security

3.2.2.10 Secure Boot Requirement

Secure Boot is part of Ford Cybersecurity strategy. For Secure Boot, obtain Preliminary Risk Assessment from the Ford Cybersecurity team on a vehicle program by program basis. Suppliers shall implement Secure Boot requirement as defined in Table 7. If the result of the Preliminary Risk Assessment mentioned above is Medium or higher.

Table 7 Secure Boot Requirement

Req. Number	Title
RQT-001403-711527	Secure Boot Requirement - Cyber security

3.2.2.11 CAN Network Gateway Requirements

Any device intended as central gateway for the CAN traffic within the vehicle (such as the Smart Datalink Connector (SDLC) or Enhanced Central Gateway (ECG)) that is interfaced directly to the CAN Diagnostic Busses (DAIG1/DAIG2) shall incorporate the Gateway Network Protection function as defined by the requirement identified in Table 8.

Table 8 CAN Network Gateway Requirements

Req. Number	Title
RQT-001403-701534	Gateway Network Protection for the Gateway Module

3.2.2.12 Advanced Operating System Requirement

Any device that leverages an advanced operating system (which includes any variety of Adaptive AUTOSAR, Linux, QNX, Windows, Android, BSD) shall meet the requirements identified in Table 9.

Table 9 Advanced Operating System Requirements

Req. Number	Title
RQT-001403-701687	Operating Systems (OS) Security Requirements

3.2.2.13 Ethernet Protocol Requirements

Any in-vehicle device that includes any of the protocols identified in Table 10 (active, inactive, future activation) shall incorporate the corresponding requirements or specification.

Table 10 Ethernet Protocol Requirements

Protocol	Req. Number	Title
SFTP	VDOC081858	In-Vehicle SFTP Security Specification
SRTP	VDOC081856	In-Vehicle SRTP Security Specification

Production software **shall never** host any of the following services under any circumstances:

- TFTP
- FTP
- Telnet
- Simple Network Management Protocol

UDP connections are strongly discouraged and will require Ford Security review and approval.

3.2.2.14 Driver Assistance and Autonomous Vehicle Sensor Requirements

Any RADAR, LIDAR, and CAMERA sensors that include an embedded system on the sensor must meet the requirements identified in Table 11.

Table 11 Sensor Security Specifications

Req. Number	Title
VDOC083309	Sensor Security Specification

3.2.2.15 Digital Key Solutions

Digital key solutions (such as Phone as a Key, NFC, CCC, or UWB) are subject to the security requirements identified in Table 12.

Table 12 Digital Key Solutions Security Requirements

Connectivity	Req. Number	Title
All	RQT-001403-704947	Vehicle Key Back-End Authentication
PaaK G1	RQT-001403-706887	Phone as a Key (PAAK) Security Controls - Cyber Security
PaaK G2	VDOC081211	BLEM Security Specification GEN 2
PaaK G2	VDOC095646	BLE Interface Security Specification GEN 2
PaaK G2	VDOC080608	Mobile App Message Security Specification
PaaK G2	VDOC080609	Mobile App Security Specification
PaaK G2	VDOC080610	Service Layer Security Specification
PaaK G3	VDOC095821	SyncP Implementation Specification for BUN Module
CCC	VDOC092979	Ford CCC Digital Key Implementation Security Specification
UWB	VDOC089495	BUN & BUNA Security Specification for Ford NFC/CCC DK
NFC	VDOC074640	Near Field Communication (Module) Security Specifications

3.2.2.16 Security Logging Requirements

All devices on the Ethernet, vehicle public can bus, or on a private CAN supporting diagnostics available at the main vehicle diagnostic connector (OBDII) shall incorporate one of the Security logging specifications identified in Table 13.

Table 13 Logging Requirements

Connectivity	Req. Number	Title
Ethernet/SOA	VDOC081373	Connected Module Security Logging Requirements
CAN/PARSED	VDOC080024	Non-Connected Module Security Logging Specification

3.2.2.17 Cryptographic Key Management Requirements

Ford Motor Company shall generate and own all cryptographic keys, exceptions should be approved by the Ford Cybersecurity Team. Key management will vary from product to product, but in general, there will be two classes of keys associated with in-vehicle modules, part number unique and serial number unique, and defined as follows:

Part Number Unique Key – A key that does not change across multiple serial numbers of the same part number. For example, if 10 modules are manufactured (serial numbers 0 to 9), then all 10 parts will contain the same key. The key inside serial number "5" will be the same as the key in serial number 2. Part number unique keys are typically public key material, such as public keys to verify signatures of software or for TLS connectivity.

Serial Number Unique Key – A key that will only be installed in a single device and will be unique for each device produced as part of the production. For example, if 10 modules are manufactured (serial numbers 0 to 9), then 10 unique keys would need to be produced and installed. The key inside serial number "5" will be different from all other serial numbers.

Part number unique keys will be provided via a manual request process from Ford unless otherwise agreed. Serial number Unique Keys and associated Ford Generated FESN will be provided via a key feed process established between Ford and the Supplier and injected at Supplier manufacturing. In general:

- Most modules will have at least one Part Number Unique Keys

- Modules that require cloud connectivity will have Serial Number Unique Keys (There are use-cases other than cloud connectivity that requires serial number unique key e.g., CMA, Secure boot etc.) Module features require authentication, authorization, and segregation of ECU boundary.

For Part Number Unique Keys, the Supplier shall take steps to prevent accidental disclosure of the key and ensure that the key is loaded into the module securely based on security specifications.

For Serial Number Unique Keys, the Supplier shall implement requirements in Table 14 and insure the following:

- Maintain key feed systems including certificates and credentials needed to obtain and consume key material from Ford.
- Key materials are protected and access is limited
- Ensure key material is injected correctly to the associated serial number at manufacture
- Produce a list of unused serial numbers (scrapped or skipped) when requested by Ford
- Immediately notify Ford in the event of key exposure, inadvertent or intentional
- Ensure that keys and FESNs are installed in only one device
- Ensure segregation between development and production intent keys. FESN Serial range for development and production are different, production key package must be provisioned into production device and dev key packages must be provisioned into dev devices only
- Must provision and manage keys and Ford Electronic Serial Numbers (FESN) based on specs listed below

Table 14 Key Management Process and Requirements/Specification

Req. Number	Title
VDOC083457	Key Packaging Specification
VDOC083458	IVSS Certificate Exchange Process
RQT-001403-724523	Key and Certificate Management Specification
RQT-001403-715043	FESN Key Request Process

3.2.2.18 In-Vehicle Connected, Web Based Cloud Requirements

Any device that is Connected, Web Engine, and Cloud based are subject to the security requirements identified in Table 15.

Table 15 Connected/Web Based Requirements

Applicable System	Req. Number	Title
Web Engine	FEA-756833	Web Application Security
Cloud	RQT-001403-705047	Vehicle to Cloud Connectivity Security
Cloud	FEA-756836	Vehicle and Mobility Cloud Security Specification
Web Engine	VDOC081280	In-Vehicle Web Application Security Requirement
Web Engine	VDOC081279	Web Engine Security Requirement
SYNC/Connected	RQT-001403-724737	Master Reset Security Specification
Ethernet	RQT-001403-704851	Ethernet Security Requirements
USB	FEA-756490	USB Security Requirements
Bluetooth	RQT-001403-704846	Bluetooth Security Requirements
WIFI	RQT-001403-704848	Wi-Fi Hotspot and AP Client Security Requirements
Ethernet	RQT-001403-724506	DOIP Security Specification
Ethernet	RQT-001403-724663	TLS 1.2 Requirements
Ethernet	VDOC086803	Service-Oriented Architecture Specification
Cloud	RQT-001403-724736	Vehicle to Cloud Security Requirements Spec

3.2.2.19 Embedded Manifest Signing Requirement

Code signing is an important mitigation mechanism to address various security risks. POSIX large file system-based modules are required to implement the requirement identified in Table 16.

Table 16 Embedded Manifest Requirement

Req. Number	Title
VDOC095102	Embedded Manifest Signing Specification

3.2.2.20 SYNCP

SyncP is a Ford approved mechanism for delivery of sensitive payloads from Ford hosted solutions with an intended delivery to a single target ECU. Cybersecurity assessment through the TARA will determine applicability of this service. Requirements for supporting SyncP functionality are listed in Table 17 in addition to the SyncP protocol Specification.

Table 17 SyncP Security Requirements

Connectivity	Req. Number	Title
SyncP	FEA-787080	Key and Certificate Management
SyncP	RQT-001403-724684	Key Rotation Security Specification

3.2.2.21 FNV4 Architecture Module Security Requirements

In addition to all other requirements listed above, FNV4 Architecture Programs shall include all applicable FNV4 requirements Table 18. Suppliers shall obtain the latest versions or additional requirements from their D&R or program contact.

Table 18 FNV4 Requirements

Applicable System	Req. Number	Title
All	RQT-001403-724826	Service $29 Authentication
OTA	RQT-001403-724664	OTA Security Requirements
Ethernet	RQT-001403-724683	TLS 1.3
HPCC	RQT-001403-724525	SOC Security Specification
HPCC	RQT-001403-724806	Hypervisor Security
HPCC	RQT-001403-723839	Container Security
HPCC/ IO Aggregator	RQT-001403-724723	Secure Time gPTP - FNV4
All	RQT-001403-724524	Secure Module Disposal Requirements
HPCC	RQT-001403-724585	Face Recognition Security Requirements In-Vehicle
All	RQT-001403-724784	Debug Token Management
HPCC	RQT-001403-724738	Intrusion Detection System Requirements
All	RQT-001403-724744	Data Privacy Assessment
All	RQT-001403-724783	Vehicle Unique Identification (VIN) Protection
HPCC	RQT-001403-724727	DNS Filtering Security Requirements
All	RQT-001403-724823	FNV4 SOA Security Requirements

Note: All modules capable of implementing service $29, shall implement service $29 instead of service $27. Refer to the cybersecurity team for service $29 applicability.

Note: FNV4 modules that implement SOA shall use the FNV4 SOA Security Requirement (RQT-001403-724823) instead of the Service-Oriented Architecture Specification (VDOC086803).

3.2.2.22 Physical Security Requirements

Depending on the product and/or service provided by Supplier, a physical security assessment may be required. Suppliers should obtain the needed documents and/or physical security requirements from their product team/engineer.

3.2.2.22.1 Gateway Equipment Physical Security Controls

Products or services that will act as a gateway by converging multiple public vehicle busses, Ethernet or CAN (Such as the Enhanced Central Gateway (ECG) and Secure Datalink Connector (SDLC)) are subject to physical assessment and physical controls. These devices shall be protected for a minimum of 5 minutes from a non-destructive (no permanent damage) attack when installed in the vehicle which may have design considerations for the Supplier. Contact the Ford Physical Security Lead to confirm required physical security controls and review of test procedure.

3.2.2.22.2 External Access Physical Security Controls

Any externally accessible (reached from outside of a locked vehicle – i.e., under body, low mounted under hood etc.) modules or harnesses with CAN connections must be firewalled or dedicated as to not allow external control of:

- Locking status
- Window motors
- Alarm
- PATS / programming keys
- Remote fobs / PaaK programming
- Keypad code programming
- Factory reset of security related modules
- Alternatively, modules / wiring identified as "at risk" may as a last resort adopt robust security shielding.

3.2.2.22.3 Mounting and Routing Physical Security Controls

Suppliers providing modules that are mounted outside of the interior of the vehicle (such as underbody, front bumper facia, rear valence, etc.) or with harnessing or connects with close proximity to perforations in the body to the exterior, shall be aware of EDS design rules (DR-180100-012069 & DR-180100-700642) and avoid installations that violate these rules. Requests to package and mount a device not in compliance with these design rules shall obtain permission from the Ford Physical Security Lead (INVEHSEC@ford.com).

3.2.2.23 AV Component Security Requirements

Autonomous Vehicle (AV) sensors not connected to the vehicle CAN are subject to the reviews, processes, and conditions defined in this SOW. The sensors shall comply with the Sensor Security Specification VDOC083309. If Implementing Diagnostic Over Internet Protocol (DOIP)/UDS, ISO 14229-5:2013 or later, the Supplier shall ensure the diagnostic services meet all requirements defined in Table 3. If not implementing DOIP/UDS, then the Supplier shall review the requirements in Table 3 and identify which do not apply and obtain approval from Ford security team before omitting the identified requirement(s).

Suppliers of these components are strongly encouraged to request a security assessment review prior to signing of the FSCA-SOW to ensure all requirements have been properly identified.

3.2.2.24 Compliance with Module or Feature Specific Specifications

The Supplier shall comply with the module or feature specific security specifications. Module or feature specific security specifications may define additional security controls for those modules that carry greater risk.

Typical modules that have these specifications include Autonomous Vehicle (AV) components, Advanced Driver Assistance Systems (ADAS), In-Vehicle Infotainment (IVI), or any feature/module with connection abilities to resources outside of the vehicle. It is the responsibility of the Supplier to confirm the applicability of module or feature specific specifications with a Ford designated security representative prior to design and implementation of such specification.

3.2.2.25 Penetration Test Planning

Penetration testing may be required depending on the product and/or service. If a previous penetration test has been completed for the product and/or service under previous sourcing and no significant hardware or software changes have occurred since such test, then another penetration test shall not be required under the current sourcing contract unless

specifically directed by Ford to complete a new test. The Supplier shall make Ford aware of the results of the previous test results and any open items affecting the current design.

Penetration testing of the product must be performed by Supplier if any of the following conditions exist:

1. The product or service falls within the criteria based on Table 19.
2. Required as part of the contract with Ford.
3. With Ford approval, the Supplier determines a penetration test is necessary to reduce risk on their product and/or service

Table 19 Penetration Test Criteria

Penetration Test Criteria	
New Connected modules/features	Connected means any module that communicates via BT, Wi-Fi or Cellular
New modules/features that communicate via RF	PEPS, RKE, Ultrasonic, Radar, NFC, DSRC, etc.
New module/service is:	In-Vehicle Infotainment System (IVI), Advanced Driver Assistance Module (ADAS), Modem or Central Gateway
Critical modules that have the following:	Several high-risk vulnerabilities identified in threat modeling or determined to be high risk by Ford.
Autonomous Vehicle Components	All new AV unique modules including VDI components, Sensors, storage modules, networking equipment, etc.…

Ford may request, at its reasonable discretion, that the Supplier conduct penetration testing for products and/or services other than as indicated in this section. In such an event, if applicable, the Supplier agrees to cooperate with Ford to conduct such penetration testing.

Penetration testing, if required, agreed, or elected, in all cases shall be executed in accordance with Section 3.10. If the Supplier has previously conducted penetration tests on the products and/or services to be delivered to Ford, the Supplier agrees to review findings from the penetration testing with Ford.

At Ford's request, the Supplier shall provide all necessary documentation and design specific componentry needed to perform penetration test activity against the design (i.e., connectors, special data acquisition systems and software, not oscilloscopes, voltmeters, etc.).

Should the Supplier elect to use a 3rd party company for the penetration testing activity, the 3rd party company chosen by the Supplier must be approved in advance by Ford.

3.2.3 Outputs

Supplier shall provide the following artifacts as a result of completing Section 3 tasks:

- Nomination of Security Lead
- Start of Progress Reporting
- Attestation to comply with Generic Security Requirements
- Attestation to comply with In-Vehicle Cybersecurity Requirements
- Attestation to comply with CAN Message Authentication Requirements
- Attestation to comply with Physical Security Requirements
- Attestation to comply with Module and/or Feature Specific Specifications
- Penetration testing plan or quote

3.3 Kickoff

The purpose of the kickoff review is to:

- Establish points of contact between the Supplier and Ford
- Ensure security requirements were appropriately communicated
- Determine Physical Security Assessment needs
- Identify if additional security specifications are necessary
- Identify key management requirements for the product or service

3.3.1 Inputs

The following artifacts are required inputs to this task:

- Nominated Security Lead
- Supplier has reviewed:
  - Program milestones and FSCA-SOW Deliverable timeline
  - Cybersecurity Requirements
  - Module Specific Cybersecurity Specifications
- Any existing Threat and Risk Model with supporting documentation for the product and/or service
- Proposal for an updated or new TARA
- Penetration test plan

3.3.2 Process

The Supplier is to schedule and lead the meeting(s) for this Initial Security Review (Kickoff). This meeting can be in the form of a WebEx or hosted on-site at the Ford offices. Other arrangements can be made as mutually agreed upon. The anticipated duration of the kick-off meeting for in-vehicle CAN based modules is approximately 1 hour. Products and/or services with additional connectivity (Ethernet, Wi-Fi, Bluetooth, cloud, etc.) or Autonomous Vehicle content may require additional time and/or meetings.

The required attendees of the Initial Security Joint Review (a.k.a. kick-off) include the following:

- Ford D&R
- Ford Security Representative
- Supplier Security Lead
- Key Supplier staff able to answer technical questions relating to the module under development

3.3.2.1 Initial Security Joint Review Topics

Topics to be covered during the meeting include, but are not limited to the following:

- Exchange of contact information between Ford Security, Ford Software, Supplier, and D&R
- Functional description of the module to be developed
- Supplier security policies or processes
- Module connectivity
- Supported features
- Review of Security Requirements and/or specifications received
- Module keying requirements (Quantity / uniqueness / algorithm / plan to provision etc.)
- Program timing and FSCA-SOW deliverable dates
- Plan to create / existing drafts of GPDS Deliverables in FSCA-SOW Toolbox from Table 2
- Overview of Product Architecture
- Review of TARA Scope and Approach
- Overview of New Connected features
- Determination of Penetration Test Plan and Scope
- Scope DV Plan

3.3.3 Outputs

Supplier shall provide the following artifacts as a result of completing the tasks in this section:

- Meeting Minutes
- Mutually agreed upon Security Requirements and Specifications
- Module Keying Approach, if applicable
- Determination of threat modeling responsibility
- FSCA-SOW delivery timing according to the program milestones
- Determination of Penetration Testing. If required, the Supplier shall; designate a responsible party, a test plan, and time it will be conducted

3.4 Module Cyber Security Plan

The Supplier shall develop a Cyber Security Plan to guide Cybersecurity development, implementation, and maintenance for the product and/or service. The Cyber Security Plan shall consider all aspects of the life cycle of each independent item, product, process and/or module. The specific content of the Cyber Security Plan will be dependent upon the type of system being analyzed. The Supplier Cyber Security plan shall be prepared, submitted, and signed off by the Supplier Cybersecurity lead and Ford. Refer to ISO/SAE 21434 Project Dependent Cybersecurity Management section 6.4.2 Cybersecurity planning.

3.4.1 Process

The purpose of the cyber security plan is to organize and plan for the cyber assurance activities throughout the duration of the product and/or service lifecycle. The Cyber Security Plan shall define the needed tasks and/or procedures to complete the project in the concept and development phases.

In general, for each cyber assurance activity, the Cyber Security Plan shall include:

- Activity goals and/or objectives
- Dependencies upon other activities or information
- Responsible party/person to complete the activity
- Resources required to complete the activity
- Start Date, End Date and duration (in days) of the activity – this should align with the corresponding GPDS and/or defined project milestones
- Identification of the corresponding work product

The Cyber Security Plan shall be updated when a change and/or a refinement of the activities to be performed has been identified. The work products required by the Cyber Security Plan shall be kept up to date throughout the project duration including development phases in order to maintain an accurate representation of the item or element, until and upon the release for production use.

In the case of distributed development (when implementation is spread across more than one organization e.g., Tier 1, Tier 2, work split), the plan shall provide the identification of the Cybersecurity activities that are to be performed by the Supplier, Ford, and/or interfaces, respectively.

The work products resulting from the Cybersecurity activities defined in the Cybersecurity plan shall be subject to configuration management and change management requirements. In the case of distributed development, the plan shall identify work products that are related to interface of distributed development.

3.4.2 Outputs

Supplier shall provide the following artifact as a result of completing this task:

- Completed Cyber Security Plan

3.5 Module Threat Analysis & Risk Assessment (TARA)

The TARA is an engineering methodology used to identify and assess cyber vulnerabilities and select countermeasures effective at mitigating those vulnerabilities. The TARA should reveal areas of potential weakness in the product or service. Refer to ISO/SAE 21434 clause 15 Threat Analysis and Risk Assessment Methods.

In compliance with UNECE WP.29 (R155), the Supplier shall complete the threat model, threat items are generated and include those identified by UNECE WP.29 (R155).

3.5.1 Inputs

The following artifacts are required inputs to this task:

- Completed Initial Review
- Agreed upon TARA Approach
- Module Keying Requirements
- Cyber Security Plan
- High-level architecture and/or existing use cases
- Functional description of item or feature
- Threat Scenario Considered UNECE WP.29 (R155)

3.5.2 Process

The Supplier shall perform a TARA or Threat Model to identify security vulnerabilities and assist risk ratings. Proposed mitigation(s) which need Ford decision must be clearly identified. Actual mitigations tied to security goals, requirements, and DVP must be traceable and shall be well documented in the TARA/threat model. This information shall be submitted by the Supplier to Ford whereby review will be performed. This review will include representatives from Ford and the Supplier as well as related subject matter experts (SME) as necessary.

The Supplier shall review and update the TARA at least once during each development cycle, (i.e., release trains), prior to the final Design Validation Plan and Report (DVP&R). In compliance with UNECE WP.29 (R155), the Supplier shall provide the threat model to Ford. Supplier will create a remediation action plan for all significant risk issues identified and submit this plan to Ford for approval. The Supplier agrees to work cooperatively with Ford to attain a level of quality and accuracy in the TARA that meets Ford's expectations.

3.5.2.1 Threat Modeling

Threat Modeling is the Threat Assessment component of TARA. There are many acceptable threat modeling methodologies. Refer to ISO/SAE 21434 clause 15 Threat Analysis and Risk Assessment Methods for examples of Threat Modeling processes. If the Supplier has not previously completed a threat model with Ford, it is strongly recommended that the Supplier schedule a threat modeling process overview. The Supplier's threat analysis shall be scoped to the boundary of the product and/or service being produced. The overview can be arranged by appointment through the Ford security team.

If no established process exists for the Supplier, Ford recommends the following methodologies:

- ISO/SAE 21434 based process
- Architectural STRIDE as implemented by Microsoft Security Development Lifecycle Threat Modeling (SDL-TM)
- Use case threat modeling
- Attack Trees
- Systems Theoretic Process Analysis (STPA)
- Hybrid threat modeling

The outcome of this process shall be:

- A detailed list of the threats of the item and/or part of the item that provides the basis for the Threat Analysis. This shall be done considering the following:
    - Each threat must have a calculated likelihood

  - Each damage scenario must have calculated impact
  - Risk must be determined using likelihood and impact
- Actual mitigations tied to security goals, requirements, and DVP must include traceable requirement numbers.
- Identify threats that are out of Supplier scope or need Ford risk acceptance
- Proposed mitigations required and/or planned to reduce the risk to an acceptable level, as determined by Ford, that shall be implemented during the design and development phases

3.5.2.1.1 Threat Modeling Objectives

The objectives of the threat modeling effort portion of the TARA are to:

- Identify design and/or implementation Weaknesses or Flaws that could manifest as Cybersecurity vulnerabilities
- Previously identified attack paths shall be updated
- Identify and document attack paths based on identified Cybersecurity vulnerabilities

The Threat Model shall:

- Document and verify all assumptions made during the analysis
- The Threat model/TARA is considered a living document and shall be updated as necessary if the design, requirements, assumptions, and/or especially the connectivity changes during the development cycle.

3.5.2.1.2 Documentation

The Supplier must review their threat model results with Ford. These results must include a prioritized list of threats. For high-risk threats, Ford requires a clear, specific, and pertinent mitigation documented for each threat. Identified threats to the vehicle should use language that clearly identifies the direct result of the exploitation of the underlying vulnerability. Avoid documenting risks that depend on many assumptions.

For example: If a module can be maliciously reprogrammed, the resulting threat to the system is the module is unable to perform the tasks it would normally perform. References to requirements and test plans are an example of a good mitigation.

If a threat was deemed not applicable or the mitigation was not implemented due to some risk, a justification must be documented and agreed upon by Ford.

If the Supplier has an existing Threat Model & Cyber Assurance documentation for the item and/or part of the item, it shall be made available for review by Ford either offline or online via a WebEx or hosted on-site at the Ford offices

3.5.2.1.3 Risk Ranking

The Supplier shall identify and list out all risks into a worksheet. The Supplier shall rate identified risks in accordance with the Cybersecurity Risk Matrix and Levels available through the FSCA-SOW Toolbox.

3.5.2.2 TARA Joint Review

The TARA Joint Review meeting can be in the form of a WebEx or hosted on-site at the Ford offices. Other arrangements may be made at the concurrence of the Supplier and Ford. The anticipated duration for in-vehicle CAN based modules is approximately one hour. Products and/or services with additional connectivity, (i.e., Ethernet, WIFI, Bluetooth, cloud, etc.), or Autonomous Vehicle content will require additional time. The Supplier is responsible for threats and mitigations of their functionality. The Supplier is responsible for scheduling the meeting with the assistance of the Ford D&R. Unless otherwise explicitly discussed and agreed upon, design changes and/or additional security controls required to mitigate or resolve the TARA security risks to an acceptable level shall be developed, incorporated, and tested as part of the original contract budget and in accordance with the GPDS program timing.

The Supplier shall host and lead the meeting. The required attendees for the TARA Joint Review include:

- Ford D&R
- Ford Cybersecurity Representative
- Supplier Security Lead

- Additional Supplier staff to support technical questions relating to the module under development

Topics to be covered during the meeting include:

- Summary of threat modeling process
- Residual risk from partially mitigated vulnerabilities

3.5.2.3 Remediation Action Plan

The Supplier shall generate a remediation action plan that addresses each unmitigated vulnerability identified during the course of the TARA. The plan shall cover proposed countermeasures that reduce the residual risk to a level acceptable by Ford and the timeline to implement. The Supplier shall review the remediation action plan and obtain approval from Ford.

Ford can request critical exposure and risk items to be mitigated on an accelerated period of less than vendor's proposed remediation/mitigation schedule. The remediation action plan shall identify changes to the design of the product or service and corresponding testing to confirm reduction of the identified risk to an acceptable level. The Remediation Action Plan shall be communicated to and agreed by Ford Security. The remediation action plan is considered a living document during the course of the development of the product or services.

3.5.3 Outputs

Supplier shall provide the following artifacts as a result of completing this task:

- TARA and Threat Models
- TARA Review Meeting(s) Minutes Captured
- Open Vulnerabilities and Action Items
- Remediation Action Plan

3.6 Module Cybersecurity Requirements

Ford reserves the right to witness all Supplier efforts to accomplish the requirements stated in the FSCA-SOW and maintains the right to approve or reject the resulting processes and/or products before implementation.

3.6.1 Inputs

The following artifacts are required inputs to this task:

- In-Vehicle Requirements and DVMs
- Module Specific Requirements
- Completed TARA
- Remediation Action Plan
- Cyber Security Plan

3.6.2 Process

The Supplier shall implement controls and mitigations that meet the In-Vehicle Cybersecurity requirements, module specific requirements, generic Cybersecurity requirements, additional controls and/or mitigations as identified during the TARA, and Remediation Action Plan in accordance with the Cyber Security Plan.

3.6.3 Outputs

The Supplier shall provide the following artifacts as a result of completing this task:

- Cybersecurity controls and/or mitigations implemented for each item identified in the TARA
- Evidence of implementation of controls and/or mitigations via inclusion of test plans and/or reports

3.7 Module Verification and Validation(V&V) Plan

A complete set of tests demonstrating compliance with all software/functional requirements, (e.g., Commodity Subsystem Specification, ECU Software Design Rules, etc.), performed on the completed software running on the target hardware will be presented by the Supplier to Ford. Refer to ISO/SAE 21434 section 10 Product Development and section 11 Cybersecurity validation.

It is intended that all tests are completed using a black-box [1]testing methodology, but it is understood that some requirements may need gray or white box tests.

If Sub-Suppliers are used to conduct design V&V testing, the Supplier shall obtain approval from Ford prior to start of such testing.

3.7.1 Inputs

The following artifacts are required inputs to this task:

- Completed TARA
- Completed implemented Requirements
- Create Functional DV Plan & Procedures and Traceability Matrix
- Perform Functional DV Test based on Functional DV Test Plan

3.7.2 Process

The Supplier shall develop a Cyber Assurance Verification and Validation (V&V) plan to guide the testing and verification of identified security controls and/or mitigations.

3.7.2.1 Cyber Assurance Verification and Validation (V&V) Plan

The Cyber Assurance V&V Plan shall cover the V&V activities for the product and/or service. The cyber assurance testing efforts shall be structured to ensure:

- Avoidance of systematic failures due to security exploits
- Control of random failures and systematic failures due to vulnerabilities or design issues
- Compliance with the Cyber Assurance requirements on all levels
- Secure operation and/or function under reasonably foreseeable circumstances
- Inclusion of all failure modes, all relevant human factor issues, and abnormal and/or infrequent modes of operation

A Cyber Assurance V&V plan shall be developed that covers:

- Tests to be conducted which addresses the items identified in the TARA
- The criteria by which the outcome of a metric will be judged as pass or fail
- A plan for missing controls and/or mitigations with timeline and responsibility for closure
- When the V&V activities are to be conducted
- Resources required to complete the V&V activities
- Assembly, calibration and/or process failures that may have an impact on testing
- Control plan with monitoring of Cyber Assurance specific characteristics.
- Data protection, collections, and privacy considerations

The Cyber Assurance V&V Plan shall be agreed upon and coordinated with Ford before the start of testing.

The Cyber Assurance V&V Plan shall be executed in accordance with the GPDS milestones as identified in Table 2.

[1] Black Box Testing is a software testing method in which the functionalities of software applications are tested without having knowledge of internal code structure, implementation details and internal paths.

All the activities stated in the Cyber Assurance V&V Plan shall be carried out as planned and shall demonstrate that all the Cyber Assurance requirements have been successfully implemented.

All activities and associated results shall be documented, or referenced, in a Cyber Assurance V&V Report

Should a change occur to a work product that has previously undergone V&V activities, the Supplier shall conduct a full impact analysis to determine if any additional regression testing is necessary. This impact analysis shall be reviewed by Ford.

3.7.2.2 Confirmation Metrics

A set of confirmation metrics demonstrating the successful implementation of the Cyber Assurance requirements shall be carried out for the item and/or part of item. These metrics shall cover the whole of the lifecycle and provide the needed evidence that the Cyber Assurance requirements have been successfully implemented. Confirmation metrics may include, but are not limited to:

- Reviews, audits, and assessments
- Analysis (Threat Models, penetration tests, code reviews, attack trees, worst case, etc.)
- Tests (function, dynamic, static, black-box, fault insertion, etc.)
- Simulations
- Vulnerability and Risk Verification on the product of service

3.7.2.3 In-Vehicle Cybersecurity Requirements Testing

The Supplier shall execute the Design Verification Methods (DVM) associated with the In-Vehicle Cybersecurity Requirements as agreed upon during the initial review in accordance with the Cyber Assurance V&V plan. The Supplier shall create the necessary detailed test procedures and present the resulting evidence unless the Test Methods are supplied by Ford. The Supplier shall make available the test procedures and resulting evidence to Ford for both created and supplied test methods.

3.7.2.4 Module Specific Cybersecurity Requirements Testing

The Supplier shall execute the Design Verification Methods (DVM) associated with the Module Specific Cybersecurity Requirements as agreed upon during the initial review in accordance with the Cyber Assurance V&V plan. The Supplier shall create the necessary detailed test procedures and present the resulting evidence unless the Test Methods are supplied by Ford. The Supplier shall make available the test procedures and resulting evidence to Ford for both created and supplied test methods.

3.7.2.5 Physical Security Requirements Testing

Unless otherwise provided, the Supplier shall develop test procedures and/or methods to validate the Physical Security Requirements as agreed during the initial review in accordance with the Cyber Assurance V&V plan. The Supplier shall create the necessary detailed test procedures and present the resulting evidence unless the Test Methods are supplied by Ford. The Supplier shall make available the test procedures and resulting evidence to Ford for both created and supplied test methods.

3.7.2.6 Remediation Action Plan Testing

The Supplier shall develop test procedures to validate risk remediation and additional security metrics identified as an outcome from the TARA review in accordance with the Cyber Assurance V&V plan. The Supplier shall create the necessary detailed test procedures and present the resulting evidence unless the Test Methods are supplied by Ford. The Supplier shall make available the test procedures and resulting evidence to Ford for both created and supplied test methods.

3.7.2.7 Code Reviews

The Supplier shall identify the necessary code reviews to confirm the successful implementation security controls and/or requirements that cannot be tested directly. The Supplier is responsible for scheduling these code reviews at least 2 weeks

in advance of projected deadline. The Supplier shall produce an appropriate agenda. Code reviews may be held via WebEx or on-site with on-site the preferred method. The Supplier shall make the source code available for inspection and provide personnel to assist during the walkthrough. If code changes are identified during the code review, the modifications shall be implemented and tested within the development lifecycle and must be complete prior to software delivery.

3.7.2.8 Cyber Assurance Test Report

The Supplier shall produce a test report documenting the results of the Cyber Assurance testing. The Cyber Assurance test report shall contain the test(s) executed, traceability information for software and hardware versions used during testing.

Sufficient information shall be recorded to allow the activities to be repeated under the same conditions (e.g. test cases, object under test, tools, environment, and test sequence).

3.7.2.9 Cyber Assurance Case

A Cyber Assurance case should be developed to show that the item and/or part of the item is secure. A Cyber Assurance case is a valid and convincing argument that the product is adequately secure for a given application. The cyber assurance case should be a summary of the Cybersecurity methodology used during the project. It should point to the efforts undertaken to establish due diligence in establishing a secure product. The assurance case summarizes the efforts and evidence generated during project lifecycle.

The Cyber Assurance Case shall include:

- Statement that threat models have been created and/or updated with any new discoveries and/or design changes as well as any new or modified risks have been adequately mitigated
- Statement from the Supplier indicating that the resulting product has mitigated known risks, has identified and communicated residual risks, and that Ford has reviewed and accepted these risks.
- Summary of efforts taken to ensure there are no known vulnerabilities in the product that has not been addressed. These efforts can include but are not limited to the following:
    - Binary scanning
    - CVE scans
    - Open software inventory
    - Penetration testing

3.7.3 Outputs

Supplier shall provide the following artifacts as a result of completing this task:

- Completed test plan
- Completed test results and reference to the test procedures followed
- Completed code reviews
- Completed Cyber Assurance Case

3.8 Initial Cybersecurity Assessment Review

The purpose of the initial Program Cybersecurity assessment review is to ensure that the D&R's have a Cybersecurity plan in place that includes adherence to the cyber deliverables, as well as awareness and adherence to requirements in FEDE. This is an internal review with Ford Vehicle Program stakeholders (e.g., D&R's, Feature Owners, and Software Leads) to review the plan and progress with respect to Cybersecurity of the critical vehicle components. Suppliers need to complete the deliverables identified before the milestone and provide to their Ford D&R for reviews. In some instances, the Supplier may be asked to support the review directly with technical or security leads.

3.8.1 Inputs

The following artifacts are required inputs to this task:

- All existing Cybersecurity work products created to date are reviewed:

- Completed Cybersecurity Relevance Assessment
- Completed Kickoff Review
- Completed Cyber Security Plan
- Completed TARA
- Completed Requirements implementation
- Completed V&V Plan

3.8.2 Process

Ensure Cybersecurity deliverables are up to date and supplied to the module D&R in advance of the review. Coordinate with the D&R and identify what personnel resources, if any, are required from the Supplier to support the review.

3.8.3 Outputs

- Meeting Minutes (if applicable)

3.9 Module Verification and Validation (V&V) Report

The Supplier shall produce a test report documenting the results of testing. The Cyber assurance test report shall contain the test executed, traceability information for software and hardware versions used during testing. The Supplier shall maintain records of the test procedures and/or methods used to allow the activities to be repeated under the same conditions, (e.g., test cases, object under test, tools, environment, and test sequences), which may be auditable. The V&V report does not need to be a dedicated Cybersecurity report meaning the report can be combined with other V&V reports of the product and/or service. Refer to ISO/SAE 21434 section 10 Product Development and section 11 Cybersecurity validation.

Inputs

The following artifacts are required inputs to this task:

- Evidence of "Passed" (successful) Test results for each Cybersecurity requirement which will include both positive and negative test cases
- Evidence of Supplier and Ford Cybersecurity sign-off for of any non-conformance to Cybersecurity requirements

3.9.1 Process

- The results of all Cybersecurity testing shall be documented, or referenced, in a Cyber Assurance V&V Report

3.9.2 Outputs

Supplier shall provide the following artifacts as a result of completing this task:

- Cyber Assurance V&V Report
- Supplier and Ford Sign-off

3.10 Penetration Testing

Penetration testing is the evaluation and assessment of the electronic control units (ECU) by safely attempting vulnerability exploitation. These vulnerabilities may exist in operating systems, services and applications and may consist of flaws, improper configurations and/or risky end-user behavior. Such assessments are also useful in validating the efficacy of defensive mechanisms, as well as end-user adherence to security policies. Refer to ISO/SAE 21434 Penetration Testing section 3.1.28 and section 11.4 Requirements and Recommendations.

3.10.1 Inputs

The following artifacts are required inputs to this task:

- Implemented and tested security controls and/or mitigations in the product

- Production intent hardware and configuration
- Requirements and Design Specifications
- Communication Protocols
- Boundary/Architecture Diagram

3.10.2 Process

The process of performing penetration (pen) tests on a system is to find common vulnerabilities and provide mitigation techniques to those specific vulnerabilities. Depending on the ECU, the Supplier shall be required to perform penetration testing. If the Supplier has not previously completed a pen test on the module, it is strongly recommended that the Supplier schedule a pen test overview with Ford Cybersecurity.

The Supplier shall propose a third party, or independent internal penetration test team, and obtain approval from Ford prior to the start of test. All Findings from the 3rd party penetration test shall be provided at Ford's request.

Testing shall be initiated along with the GPDS Milestone <DCV> and shall be completed with sufficient time to incorporate remediation prior to GPDS milestone <TT>. The Supplier must fix or remediate to Ford satisfaction any Cybersecurity issues identified as part of the pen test at their cost.

The Supplier is to schedule and lead a meeting for this Initial Security Review. This meeting shall be hosted on-site at the Ford offices. If features are added later, (such as a post <J1> OTA update), that changes the threat model, a delta penetration test may be required to evaluate the added functionality.

3.10.3 Outputs

Supplier shall provide the following artifacts as a result of completing this task:

- Penetration Test Results
- Penetration Test review
- Vulnerability Report
- Remediation Plan
- Updates to TARA
- Unfiltered results from pen testing

3.11 Final Cybersecurity Assessment Review

The purpose of the final Cybersecurity assessment review is to ensure that the D&R's have completed a Cybersecurity plan in place that includes adherence to the cyber deliverables, as well as awareness and adherence to requirements in FEDE. This is an internal review with Ford Vehicle Program stakeholders (e.g., D&R's, Feature Owners, and Software Leads) to review the plan and progress with respect to Cybersecurity of the critical vehicle components. Suppliers need to complete the deliverables identified before the milestone and provide to their Ford D&R for reviews. In some instances, the Supplier may be asked to support the review directly with technical or security leads.

3.11.1 Inputs

The following artifacts are required inputs to this task:

- Cybersecurity Relevancy Assessment form completed
- TARA documentation showing evidence that all identified gaps have been closed complete
- Evidence showing identified Cybersecurity issues are closed and related functional specifications have been updated with new Cybersecurity requirements
- Penetration Test(s) completed, and gaps addressed (if applicable)
- Cybersecurity V&V Reports completed and passed
- Consensus is reached on plans to resolve any Cybersecurity related non-conformances with appropriate sign-off
- Post-production Cybersecurity requirements documented
- Cybersecurity Case rationale identifying state of achieved Cybersecurity documented

- All evidence stored appropriately in VSEM

3.11.2 Process

Ensure that all Cybersecurity documentation is complete. This includes ensuring that all evidence is stored appropriately in VSEM and that the Cybersecurity Case (rationale identifying state of achieved Cybersecurity) is documented, reviewed, and stored.

3.11.3 Outputs

Ford to proceed to next milestone.

4 General Cybersecurity Requirements

The clauses in this section apply to all Cyber Assurance related efforts (e.g., Threat Model, Cyber Assurance Checklist, schedules, specifications, descriptions, technical reports of risks, threats, security cost trade-off, impact analyses, status reports, models and/or other documents).

Post Job One (J1) Support

As Cybersecurity risks evolve over the course of the product or service lifecycle, some cyber assurance tasks extend beyond the development phase. Suppliers shall monitor for Cybersecurity vulnerabilities and exploits that relate to Supplier's Goods, Tech Products, or Services throughout the duration of supply and use in Ford vehicles of such Goods, Tech Products, or Services to Ford.

4.1 Road Vehicles — Cybersecurity Engineering

The Supplier shall comply with ISO/SAE 21434 Road Vehicles Cybersecurity Engineering. ISO/SAE 21434 specifies requirements for Cybersecurity risk management regarding engineering for concept, development, production, operation, maintenance, and decommissioning for road vehicle electrical and electronic (E/E) systems, including their components and interfaces.

ISO/SAE 21434 is meant to supersede SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. It expands on the same concepts and Cybersecurity due diligence. All Suppliers are meant to become familiar with the standard as Ford expects Supplier adherence to this standard and new UNECE Cybersecurity Regulations. Suppliers must provide Threat Analysis and Risk Assessments (TARA) of their products, have ability to triage vulnerabilities, if found, and be able to track compliance to requirements throughout their lifecycle processes. Supplier evidence and processes required as part of this FSCA-SOW shall be compliant with ISO/SAE 21434 and UNECE ECE/TRANS/WP.29 R155. Ford reserves the right to request inspections, review internal audits, inspect documentation and evidence in support of UNECE R155/R156 and ISO/SAE 21434Witness of Testing and Inspection of Results.

Ford reserves the right to review and right to witness all Supplier efforts to accomplish the requirements stated in the FSCA-SOW and maintains the right to approve or reject the resulting processes and/or products before they are implemented.

4.2 Third-Party Testing

Ford may require additional testing, or the Supplier may elect to employ additional testing as means for risk reduction. The Supplier shall notify Ford and obtain approval prior to contracting third-party testing. Ford recommends Secure Code Reviews, Fuzz Testing and other input validation testing, and Penetration Tests and/or Red Team assessments.

4.3 Documentation

Supplier shall perform and provide evidence to Ford that due diligence has been performed regarding the planning, implementation, and testing of all aspects relevant to Cyber Assurance activities.

- The Supplier should track warranty returns and provide Ford necessary data and analysis details upon request.

4.4 Supplier Deliverables

The following requirements apply to all deliverables covered by the FSCA-SOW. All deliverables shall be:

- Delivered and accepted by the program milestone identified
- Supplied in English and in electronic format
- Propose and get confirmation of document structure at project start
- The Supplier shall make available in electronic format a copy of the source code and other relevant design documentation available to Ford to support code reviews and static analysis verification.
- The Supplier shall provide unit test procedures and/or methods along with the results for review by Ford upon request.

- The Supplier shall provide system/integration test procedures and/or methods for all features.

4.5 Production-Ready Security State

The Supplier shall ensure that all known security defeating techniques or development tools or any technology used during the development and diagnostics of the product, process, or module will be disclosed to Ford and disabled prior to production. This includes but is not limited to:

- Include flags that load and/or execute values based on the module being in development phase vs. production phase
- Insecure, plain text, or hardcoded keys and/or passwords
- Unlock codes allowing arbitrary unsigned code loading and/or execution
- Disable or implement a challenge mechanism (e.g., password protection) on hardware debug interfaces

A failure to do so may constitute a recall or a Field Service Action at the Supplier's expense.

4.6 Information Sharing/Vulnerability, Exploit, and Incident Disclosure

The Supplier shall notify Ford if they become aware of a vulnerability and/or exploit affecting the product as indicated below. The Supplier shall:

- Support discussions to determine the impact, formulate Interim Corrective Actions, and/or Permanent Corrective Actions to address the vulnerability or exploit
- Perform an investigation to determine the root cause leading to the vulnerability or exploit and propose methods to protect against similar issues in future products
- Produce manufacturing data, (serial numbers, production numbers, manufacturing facilities, etc.), necessary to identify impacted vehicles at Ford's request
- Notify Ford within 30 days of becoming aware of the issue, even if investigation is still on-going

This requirement applies to vulnerabilities and/or exploits discovered at any time, including after manufacturing.

4.7 Published Vulnerabilities Resolution

The Supplier shall patch or remediate any published or pending vulnerabilities affecting the product and/or service as published in the MITRE Common Vulnerabilities and Exposures (CVE) or NIST National Vulnerability Database (NVD) with a CVSS score of 7 (High) fix and address prior to J1. Any CVSS score of 4.0 (Medium) or greater prior to production software release will be investigated individually for the associated risk and determine next steps. Any vulnerabilities with a CVSS score of 3.9 (low) or lower shall be disclosed and reviewed with Ford. Other known published vulnerabilities (with or without an accompanying CVSS) shall be disclosed to Ford with accompanying planned countermeasures and/or mitigations.

CVEs identified affecting software in production shall immediately notify Ford via the Ford Incident Response Triage Process (See Section 4.8) and the Ford security lead for the affected product(s). The Supplier shall coordinate with Ford on appropriate remediation strategy and, if within the warranty period, release a software update. If the vulnerability affects software delivered by a Sub-Supplier, the Tier 1 is responsible to coordinate the remediation through the business agreements between the Tier 1 and Sub-Supplier.

4.8 Ford Incident Response Triage Process

Ford can be contacted via several different ways depending on who is providing vulnerability information. If the Supplier becomes aware of a vulnerability, exploit and/or another incident, the Supplier shall:

- During development - Coordinate with Ford security lead.
- After development or in a fielded product – Immediately notify the Ford security lead or CIRT@ford.com. For CIRT@ford.com, if no response within sixty minutes, call U.S. (313) 580-6328.

4.9 Sub-Supplier(s)

A Sub-Supplier is a vendor or consultant who provides goods or services to the Supplier. Ford reserves the right to request this evidence if sub-Supplier(s) are used to provide cyber-relevant components or software, the Supplier shall:

- Notify Ford of the sub-Supplier and their role in the product development lifecycle and/or production
- Include the requirements in this FSCA-SOW in Supplier's contract with the sub-Supplier
- Identify the sub-Supplier activities in the Cyber Security Plan
- Ensure that the sub-Supplier responds independently to information requests. Completed responses should be returned to the requested Supplier
- Collect all sub-Supplier responses, which should be attached as supporting documentation and be submitted to Ford for review
- Supply documentation to support compliance with all requirements in this document
- Describe the methods, deliverables, persons by which the sub-Supplier will interface with the Supplier Cyber Security Plan
- Specify the contact details for the Sub-Supplier (Name, Phone, Email, Title, and corporate affiliation)
- Be responsible for software produced by the sub-Supplier

Such testing shall be incorporated into the Acceptance Test Plan to be submitted to Ford for approval. Verification failures found during sub-Supplier testing may result in the Supplier's verification test plan being rejected. In such circumstances, the Supplier will amend the plan and conduct any additional testing at its cost.

4.10 Secure Coding Practices

Suppliers shall utilize Secure Coding Practices, perform static code analysis reviews, and should follow industry standards such as MISRA or CERT-C on products and processes. Refer to Global ESOW Software for more guidance on secure coding practices.

4.11 Cryptographic Export Documentation

The Supplier shall determine if there are any regulatory concerns regarding technology used in the production of this module related to cryptographic exports to the intended markets (i.e., China's Cryptographic Law). All components shall follow appropriate import/export requirements for the use of cryptography within a product. All use of cryptography shall be documented for Ford Legal reference.

4.12 Protection of Cryptographic Keys

The Supplier shall implement a solution ensuring symmetric keys, private keys in the case of asymmetric cryptographic algorithms, and private certificates are protected from disclosure and modification in secure storage (e.g., HSM/SHE). Obfuscation is not adequate to meet this requirement. Any other solutions to protect private keys shall be reviewed and approved by Ford.

Public keys shall be protected from modification. Note: protection of public keys, such as those used for application signing or secure boot, do NOT require secure storage protected by an HSM/SHE.

4.13 Connected Vehicle Technology

If the product or service is planned to exchange data over a network connection outside of the vehicle for any reason, security discussions with Ford Cybersecurity are required. This includes Ethernet traffic to be exchanged through the gateway and onboard modem. Isolation and security controls for protection of the data over the network must be documented and mutually agreed upon.

4.14 Cyber Assurance Reviews

Additional cyber assurance reviews may be necessary beyond the initial review, TARA review, code reviews, and final review. Ford may request additional cyber assurance assessment during the development of security controls. The Supplier shall support with appropriate preparation and staffing. Supplier may be at Ford's premises.

A typical Cyber Assurance assessment will cover the following:

- Agenda for the assessment
- Work done since the previous Cyber Assurance Review
- Recommendations of the previous Cyber Assurance Reviews and/or Remediation Plan
- Tools that are used as part of the design, implementation and/or test
- Exchange of technical data and procedural information to support securing the product or service
- Test procedures, methods and/or additional reviews necessary to address risk remediation identified as part of the assessment

The Supplier shall document the results of the assessment in a Cyber Assurance Reviews report. The Cybersecurity test plan and procedures and/or methods shall be updated to reflect design changes and/or additional controls as agreed to as part of the Cyber Assurance Assessments.

4.15 Open-Source Software

The Supplier is responsible for the integrity and proper licensing of all software libraries or components delivered (licensed or from open source). Specifically, the Supplier shall execute the following duties when incorporating open-source software into their product:

- Identify and provide documentation of open-source libraries and version incorporated into the product and all required dependencies
- Ensure licenses associated with open-source components are compatible with intended use in the final product and explicitly do not contain components with licenses that have conditions that trigger upon distribution (e.g., GPL, AGPL). Confer with Ford as to application of specific open-source license to the product.
- Ensure all identified vulnerabilities relating to the version of the library or component have been patched or removed
- Only binaries and libraries explicitly used by the production image shall remain in the final image. Debugging or unused libraries shall be removed.
- Maintain audit trails of program changes, program version numbers, creation-date information and copies of previous versions and/or evidence for proper licensing
- Maintain archived copies of the source used for the product in the event that the original source becomes no longer accessible
- Immediately notify Ford if Supplier becomes aware of a published vulnerability in a product or service in a planned or released production binary

This covers all software managed by the Supplier as well as included in third party or sub-Supplier provided software, whether in source or binary forms. Refer to the Global ESOW Software attachment for additional guidance on licensing of third-party software.

4.16 Software Bill of Materials (SBOM)

A software bill of materials (SBOM) is a key part of software security and software supply chain risk management. A SBOM is a nested inventory, a list of ingredients that make up software components. Any cyber relevant modules incorporating a POSIX OS (Unix, Linux, Android, QNX, Adaptive AUTOSAR, or variants on these) software or Ethernet Connected. For AutoSAR modules, this submission can be optional if the Supplier attests that no Open-Source Software (OSS) or third-party software components other than those provided by the AutoSAR Supplier or Ford are leveraged. The SBOM may be

composed using automated tooling (Eg. Source code or binary scanning) or other techniques. The SBOM shall be reported in an industry standard format (e.g. SPDX, CycloneDX, SWID) as mutually agreed by Ford and the Supplier.

4.17 Cybersecurity Triage Support

In the event Ford becomes aware of a cybersecurity vulnerability or incident affecting the product or service, Ford will issue a request to the Supplier for investigation in support of triage. The Supplier shall respond within 30 days of the request or sooner. The Supplier shall support discussion and initiate internal triage process and support Ford in determining best case remediation.

4.18 Cybersecurity Monitoring

The Supplier shall have a process for monitoring cybersecurity vulnerabilities or incidents affecting their product or service. This section also applies to Ford's (or the Supplier's) IP, Cryptographic material, or PII being compromised. Once a vulnerability or incident is confirmed, The Supplier shall notify Ford in accordance with Section 4.7.

4.19 Support of Architecture/Vehicle Threat Model

On request, the Supplier shall support Ford in developing the vehicle level threat model. This support will consist of meetings and communications (emails, documents, etc..) regarding vulnerabilities uncontained by the individual component, or service, and requiring remediation at a system level.

Appendix A. Contact Details

Contact	Contact Detail
Ford FSCA-SOW Contact	FSCA-SOW
Ford Software Signing Contact	Software Signing
Ford CAN Message Authentication Contact	CAN Message Authentication
Ford Threat Model Contact	Threat Modeling
Ford Point of Contact	Refer to your Ford D&R

Appendix B. Cybersecurity Interface Agreement

The entries of column are:

- "Task" – Name of the Task or Work product
- "FMC" – Ford and "SE" – Supplier. Defined as Follows:
  - R (Responsible): The organization that is responsible to conduct the activity
  - A (Accountable): The organization that has the authority to approve the activity once it is complete
  - S (Supporting): The organization that will help the organization responsible for the activity
  - I (Informed): The organization that is informed of the progress of the activity and any decisions being made
  - C (Consulted): The organization that offers advice or guidance but does not actively work on the activity

The "FMC" and "SE" column R/A/S/I/C designation may be changed or amended with Ford Approval.

Task	Ford	Supplier
Module Cybersecurity Relevance Assessment		
Complete Ford Internal Relevance Assessment	R, A	I
Contract Award		
Identify Security Leads	I	R, A
Kickoff		
Determination of TARA Scope and Approach	A	R
Determination of Penetration Test	A	R
Obtain and review relevant In-Vehicle Cybersecurity Requirements	C	R, A
Module Cyber Security Plan		
Develop and deliver Cyber Security Plan	A	R
Module TARA		
Create the Item Definition	I	R, A
Execute the Threat Model	I	R, A
Review TARA with Ford	A	R, A
Develop and obtain approval for any Remediation Action Plans	A	R, A
Module Cybersecurity Requirements		
Implement Cybersecurity Requirements	I	R, A
Module Verification and Validation Plan		
Create the V&V plan	A	R
Initial Cybersecurity Assessment		
Hold Initial Cybersecurity Assessment with Ford	R, A	S
Module Verification and Validation Report		
Gather evidence of test results	I	R, A
Review evidence cybersecurity sign-off with Ford	A	R
Complete Cyber Assurance V&V Report	I	R, A
Penetration Testing		
Review test results with Ford	A	R
Final Cybersecurity Assessment		
Cyber Assurance Case generated, and delivered	I	R, A
General Cybersecurity Requirements		
Road Vehicles — Cybersecurity Engineering	I	R, A
Witness of Testing	R	A
Inspection of Results	R	A
Third Party Testing	I	R, A
Supplier Deliverables	I	R, A
Production Ready Security State	I	R, A
Information Sharing/Vulnerability, Exploit, and Incident Disclosure	I	R, A
Published Vulnerabilities Resolution	I	R, A

Task	Ford	Supplier
Sub-Supplier(s)	I	R, A
Secure Coding Practices	I	R, A
Cryptographic Export Documentation	I	R, A
Protection of Cryptographic Keys	I	R, A
Cyber Assurance Reviews	I	R, A
Open-Source Software	I	R, A

Appendix C. Terminology and Abbreviation

Abbreviation	Description
ADAS	Advanced Driver Assistance Systems
AGPL	Affero General Public License
AV	Autonomous Vehicle
Cyber Assurance	The justified confidence that networked systems including hardware, software, and communications are adequately secure to meet operational needs, even in the presence of attacks, failures, accidents, and unexpected events
CCC	Car Connectivity Consortium
CCMC	CMA Change Management Committee
CDC	Cyber Defence Center
CMA	CAN Message authentication
CVSS	
BSD	Berkeley Software Distribution
D&R	Design and Release
DCR	Design Change Request
DCV	Development Completion Vehicle
Developmental SW	Software in the design process, but not validated or released
DIA	Design Interface Agreement
DK	Digital Key
DR	Design Requirement
DSRC	Dedicated Short Range Communication
DV	Design Verification
ECU	Electronic Control Units
EDS	Electrical Distribution System
Exposure	Vulnerability without a control
FDJ	Final Data Judgement
FEC	Final Engineering Completion
FEDE	Ford Engineering Design Environment
FESN	Ford Electronic Serial Number
FNV	Fully Networked Vehicle
FSCA-SOW	Ford Supplier Cyber Assurance - Statement of Work or this document
Fuzz Testing	Also called “Fuzzing” is a software testing technique used to discover coding errors and security loopholes in software, operating systems or networks by inputting massive amounts of random data, called fuzz, to the system in an attempt to make it crash.
GPDS	Global Product Development System
GPL	General Public License
HPCC	High Performance Compute Cluster
HSM	Hardware Security Module

Abbreviation	Description
I-Build	Integration Build - An iterative system integration process implemented in parallel with the GPDS design phase (PSC – FDJ). This process is intended to verify base software technologies and to confirm basic system compatibility prior to production design completion.
IOA	Input/Output Aggregator
IVI	In-Vehicle Infotainment
J1	Job 1
MISRA	Motor Industry Software Reliability Association
NFC	Near Field Communications
Open Source	Software for which the original source code is made freely available and may be redistributed and modified
PEC	Preliminary Engineering Completion
Penetration Test	Also called "Pen testing" is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.
PEPS	Passive Entry Passive Start
POC	Point of Contact
PS	Program Start
PSC	Program Strategy Confirmed
Risk Matrix	A Risk Matrix is a matrix that is used during Risk Assessment to define the various levels of risk as the product of the harm probability categories and harm severity categories. This is a simple mechanism to increase visibility of risks and assist management decision making
Secure Code Review	The process which identifies the insecure piece of code which may cause a potential vulnerability in a later stage of the software development process, ultimately leading to an insecure application.
SHE	Secure Hardware Extension
STRIDE	STRIDE Methodology is a system developed by Microsoft for thinking about computer security threats. The threat categories are: Spoofing of user identity, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
TAC	Technical Assistance Center
TARA	Threat Assessment and Risk Analysis
Threat Modeling	A procedure for optimizing network security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system.
TSC	Technology Strategy Confirmed
UNV0	Underbody Verification 0
UNV2	Underbody Verification 2
UPV0	Upperbody Verification 0
UPV2	Upperbody Verification 2
UWB	Ultra-Wideband
V&V	Verification and validation
Vulnerabilities	Part of the information security infrastructure that could represent a weakness to attack in the absence of a control. Constitutes but is not limited to CVE database published by CERT