

CG4211
SQ Security of Software for Supplier Manufacturing SOR Appendix F

Document Owner: Gildardo Mariano

Author: Arthur Fung

Revision: 7 – September 9, 2019

Herein are the minimum requirements that shall be incorporated into the manufacturing process for the above commodity. NOTE: This Part Specific SOR is in addition to and not intended to replace any requirements as outlined in the GM Supplier Quality SOR (GM-1927-03). It is understood that advances in technology may require modifications to the following requirements to ensure state of the art processing and testing. It is the responsibility of the supplier to ensure that the process is state of the art and that the GM SQE is both informed and in agreement to any modifications of the requirements below.

The required tasks indicated below are based on lessons learned to improve part quality using APQP Continuous Improvement activity in GM projects and are applicable to all impacted suppliers and parts in the supply chain. All deviations requested for “shall” items are to be detailed in CG3404 M7 Technical Issues List found in eSOR Appendix M7, and reviewed and approved by General Motors Supplier Quality prior to sourcing.

“Shall” in this document is mandatory. “Should” is highly recommended. Supplier confirms that products sold to GM will be produced and supported under the following requirements. “*Electronic Devices*” refers to any object, machine, or piece of equipment that is used to store or process sensitive electronic information. “*Business Enterprise Location*” refers to any facility (manufacturing, sales, distribution, engineering, etc.) involved in the design, manufacture and distribution of the product delivered to GM.

1. Business Enterprise Locations

- 1.1. A full-time employee or subcontracted IT security staff shall be available within 24 hours.
- 1.2. An appropriate computer security education and awareness program shall be available to all employees and part of the standard training package.
- 1.3. An automated method of detecting and blocking malicious e-mail prior to delivery shall be in place.
- 1.4. A Computer Incident Response process to respond to cyber-attacks shall be in place at each location.
- 1.5. The use of automated tools and processes to mitigate Advanced Persistent Threat (APT) attacks shall be in place. Notification of any occurrences or attacks shall be communicated to GM.
- 1.6. Access to high-risk (e.g. reputation, content, and security) sites shall be restricted.
- 1.7. Exchanging sensitive information (as defined in appendix B – Glossary) with any other organization or business enterprise shall follow procedures for cyber security based on industry standards (e.g. ISO 27001, NIST 800-53).
- 1.8. As instructed by the GM Information Systems Innovation team, a review of the “*Third Party Information Security Requirements*” (TPISR) shall be completed by the supplier and any concerns reviewed and documented.
 - 1.8.1. Requests for additional information can be directed to GM_Third_party_security_program@gm.com.
- 1.9. The supplier shall communicate to GM Supplier Quality any Cybersecurity-related incidents within the manufacturing operations within 48 hours of detection.
- 1.10. Personal e-mail accounts shall not be used for business purposes with General Motors
- 1.11. Cloud based services shall be approved by GM Information Security.

2. Business Enterprise Devices

- 2.1. The use of Personal Electronic Devices shall not be allowed to access GM information unless additional security measures are in place. These measures shall be reviewed and approved by the appropriate GM cyber security personnel.
- 2.2. Access control for all *Electronic Devices* and/or IT services shall be configured using the “least privilege model” (a person only has access to the data/device that they need).
- 2.3. *Electronic Devices* shall have a unique user name and complex password to access the system.
- 2.4. *Electronic Devices* shall have vulnerability scanning (i.e. Coverity, Protocode, etc.) performed at least monthly, and the vulnerabilities are remediated in a risk based priority report, with the highest priority vulnerabilities being fixed first. The report shall be available to the SQE upon request.
- 2.5. *Electronic Devices* shall have unnecessary ports and services disabled when used for limited functions such as when a device acts 1) solely as a file server versus 2) acting as file server / FTP server / web server.
- 2.6. *Electronic Devices* shall have commercially available antivirus and malware detection programs installed and updated regularly.

CG4211

SQ Security of Software for Supplier Manufacturing SOR Appendix F

Document Owner: Gildardo Mariano

Author: Arthur Fung

Revision: 7 – September 9, 2019

- 2.7. *Electronic Devices* that store or process a third-party company's sensitive information shall be protected from the Internet by a firewall.
- 2.8. *Electronic Devices* capable of transferring sensitive information shall be encrypted.
- 2.9. A 2-factor authentication process for an *Electronic Device* to gain remote access shall be utilized. Allowing the system to remember the device should not be allowed.
- 2.10. Mobile *Electronic Devices* (e.g. smartphones, tablets) shall have mobile device management (MDM) provided by a company owned centrally managed infrastructure and have access controlled by a complex password.
- 2.11. Unsecured public Wi-Fi shall not be used to communicate with GM unless a Virtual Private Network (VPN) is utilized.
- 2.12. When using Portable Electronic Devices, the feature of remembering user name and password shall not be allowed.

3. Equipment Maintenance

- 3.1. Before any new *Electronic Device* is installed or able to access the local network, it should be subjected to an established and proven antivirus program, and any suspect files removed. A risk assessment shall be conducted to determine high-risk devices that shall be subjected to the antivirus program.
- 3.2. Before any *Electronic Device* being repaired is put back "on-line", it shall be subjected to an antivirus program, and any suspect files removed.

4. Shipping & Logistics

- 4.1. Any wireless (i.e. Wi-Fi, Bluetooth, etc.) based *Electronic Devices* used in supply chain logistics shall have internal firewall protection for device-to-device communication. Wireless based devices shall have internal firewall protection.

5. Incoming Inspection and Finished Goods Audits

- 5.1. A sample from each shipment of incoming components that contain pre-loaded software / firmware shall be subjected to an established and proven antivirus program, and if suspect files detected, the entire shipment shall be quarantined.
- 5.2. Samples from lot codes of all finished goods modules & assemblies that contain software shall be subjected to an antivirus program, and if suspect files detected, the entire lot code shall be quarantined.

CG4211
SQ Security of Software for Supplier Manufacturing SOR Appendix F

Document Owner: Gildardo Mariano
 Author: Arthur Fung
 Revision: 7 – September 9, 2019

Appendix A – Revision History

Rev	Date	Remark	Responsible	Approver	Approving Organization
A (1)	11/3/2014	Initial release	John Mason	Damon Salisbury	Supplier Quality
B (2)	8/8/2115	Changed supplier to business enterprise, Relabeled sections to B.E. locations and B.E. devices and renumbered. Added personal device usage. Created appendix A for approvals.	John Mason	Damon Salisbury	Supplier Quality
C (3)	11/20/15	1. Revised items 1.2, 1.4, 1.5, 1.8, 2.10, 3.1, 4.1 2. Removed Appendix A: supplier signature & exception approval page 3. Updated Revision history from Appendix B to Appendix A	John Mason	Damon Salisbury	Supplier Quality
D (4)	8/1/16	1. Revised wording of section 1.8 2. Added Malware detection in section 2.6	John Mason	Damon Salisbury	Supplier Quality
E (5)	1/18/18	1. Revised wording of items 1.2, 1.6, 1.8 & 1.9 2. Added items 1.10 & 1.11 3. Revised wording of items 2.1, 2.4, 2.5 4. Added items 2.11 & 2.12 5. Revised wording of items 3.1, 4.1, 5.1 6. Updated glossary	John Mason	Damon Salisbury	Supplier Quality
6	6/6/2019	1. Updated item 1.8 regarding TPISR	Arthur Fung	Damon Salisbury	Supplier Quality
7	9/9/2019	Changed document owner to Gildardo Mariano	Gildardo Mariano	Gildardo Mariano	Supplier Quality

CG4211

SQ Security of Software for Supplier Manufacturing SOR Appendix F

Document Owner: Gildardo Mariano

Author: Arthur Fung

Revision: 7 – September 9, 2019

Appendix B – Glossary

GM Information: All information, physical and electronic or otherwise, relating to the business of GM and created or acquired using its resources or interacting with GM personnel. All GM Information is the sole property of GM. GM Information exists in many forms, including but not limited to product plans, vehicle designs, product prototypes, strategy documents, business records, pricing information, financial or technical data, marketing information and text, sound or image files.

Complex Password: A mix of uppercase, lowercase and numeric characters, where technically capable. The use of special characters is authorized

Electronic Devices: Any object, machine, or piece of equipment that is used to store or process sensitive electronic information.

Business Enterprise Location: Any facility (manufacturing, sales, distribution, engineering, etc.) involved in the design, manufacture and distribution of the product delivered to GM.

GM Third Party Information Security Requirements (TPISR): A set of security requirements that applies to all Third Parties who collect, process, manage, access, or store GM Information, external to the GM computing environment, and to those who provide critical goods or services to GM. The TPISR is designed to be a set of nonprescriptive, technology independent, minimum-security requirements for new GM agreements.

Personal Electronic Devices: Any piece of lightweight, electrically powered equipment such as laptop pc's, tablets, e-readers, and smartphones.

Third Party: A company, business, organization, supplier, or group that conducts business with, provides goods or services to, directly or indirectly, to General Motors. These entities may create, collect, manage, process, store, transmit GM Information, or represent GM in the course of business.