Cyber Security Framework for Autonomous Machines

Principal Author: Dr. Edward G. Amoroso

Chief Executive Officer, TAG Cyber LLC

eamoroso@tag-cyber.com

Version 1.0

September 18, 2018

Abstract

This *Cyber Security Framework for Autonomous Machines* is offered as a high-level security and compliance requirements guide for developers creating autonomous machines including future connected cars, robots, medical devices, and industrial controllers. The framework is written in an abstract manner so that it can address each of these diverse areas without imposing specific design decisions. The framework is written in the style of the *NIST 800-53 Rev 4 Cybersecurity Framework* to simplify its application and use, perhaps as an appendix to any NIST assessment for a computing entity with autonomous machine characteristics.

Introduction

An *autonomous machine* is a computing entity consisting of hardware, software, and communication interfaces that accomplishes a set of desired functions without requiring assistance from human beings. Self-driving cars represent one of the more commonly-cited examples of autonomous machines. Human involvement with autonomous machines is limited to programming, provisioning, protocol interaction, remote update, and de-provisioning. The autonomous machine dynamically self-controls real-time and on-going interactions with its environment, including local decisions about how to collect incoming stimuli, how to interpret such data, and how to initiate actions.

The distinction between an autonomous machine and its environment is subtle, because the functional operation of any modern computing entity could include interaction with remote capabilities, such as might be found in a cloud computing system. The autonomous machine is thus viewed as the minimal set of processing, memory, and input/output functions required to accomplish its mission. If such functions are scattered physically across virtual infrastructure, then this does not change the underlying autonomy of the machine. This framework thus references autonomous machines independently of their specific implementation, distributed or otherwise.

Cyber security requirements for various types of autonomous machines are currently being developed in a variety of specific areas around the world. For example, the SAE Vehicle Electrical System Security Committee is developing security requirements guidebook that focuses specifically on a set of detailed controls. This report, in contrast, focuses more generally on the cyber security aspects of autonomy and self-control of machines, under the assumption that such autonomy introduces functional issues such as maintenance of a set of common beliefs and norms, as an autonomous machine makes decisions.[1]

A general model for autonomous machines and how they interact with their manufacturer, their functional environment, and other autonomous machines is provided in Figure 1.

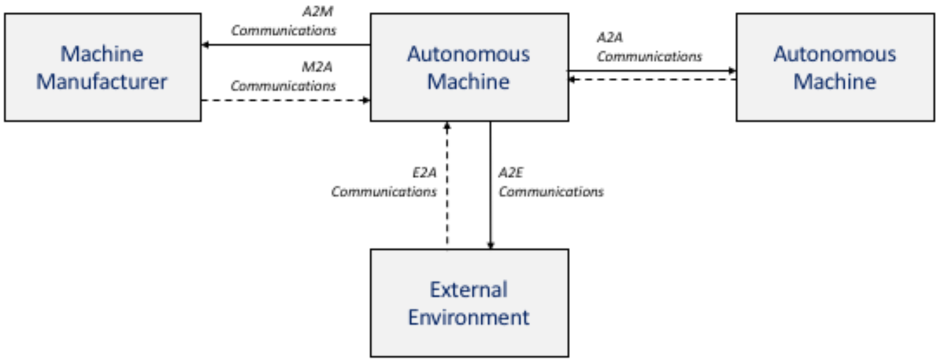

Figure 1. Model of an Autonomous Machine

The processing, data handling, computation, and network interactions for an autonomous machine will involve its manufacturer, environment, and other autonomous machines. This implies three types of operational entities that will require cyber security protection: Manufacturer, autonomous machine, and environment. It also implies five types of communication interactions that will require cyber security protection: Autonomous machine to manufacturer (A2M), manufacturer to autonomous machine (M2A), autonomous machine to autonomous machine (A2A), autonomous machine to environment (A2E), and environment to autonomous machine (E2A). The goal in each case is to ensure prevention of unauthorized disclosure, integrity-reducing interactions or modifications, and denial of service.

The purpose of this framework is to introduce cyber security requirements that human designers must enforce in the design, development, provisioning, management, update, interaction, and de-provisioning of autonomous machines. Since autonomous machines might make insecure decisions, a security framework is thus required to guide all functional and procedural outcomes to ensure that policy violations do not occur. To support local self-control and autonomy, such framework involves establishing foundational principles that are immutable; it also includes policy decisions that can be modified – so long as they maintain consistency with principles; and finally, it includes set of functional controls that protect the autonomous machine from external, environment threats.

[1] The term "autonomous machine" was selected rather than "autonomous system" to avoid conflict with the familiar notion of an autonomous system (AS) as a collection of Internet protocol prefixes under common management.

The requirements definition style follows the familiar NIST 800-53 Rev 4 issuance to help autonomous machine designers understand how to apply the framework. Each requirement below is defined in the context of the model of an autonomous machine shown above, as well as an outline for how an assessor would determine compliance with the designated requirement. Audit and regulatory teams might choose to cut-and-paste this framework as an appendix to the NIST framework, should these requirements match the autonomous mission of whatever system is being investigated.

1. Security Requirements for Manufacturers

Manufacturers of autonomous machines should maintain compliance with the following cyber security requirements:

1.1 Foundational Security Principle Issuance

"Manufacturers must create a foundational belief structure for autonomous machines."

Control Requirement: The autonomous machine shall be provisioned by its manufacturer with a set of security foundation principles that serve as an immutable belief structure that cannot be altered by the autonomous machine, external environment, human users of the autonomous machine, or any other autonomous machines for any reason. Foundational principles shall be based on local standards, customs, laws, and norms. If the manufacturer chooses to change foundational security principles, then this can only be done through retirement and re-deployment of the autonomous machine with new foundational principles.

Control Compliance: The autonomous machine assessor shall determine compliance with this control requirement based on the following tests:

- **Provisioned Principles:** The security foundational principles shall be shown to be included in the provisioning process.
- **Immutability Testing:** Security and penetration testing shall be performed to demonstrate immutability of stored principles.
- **Immutability Design Review:** Reviews of autonomous machine design shall be performed to confirm that mechanisms are in place to prevent changes to the security principles.

1.2 Initial Security Policy Issuance

"Autonomous machines must accept an initial set of security policy rules."

Control Requirement: The autonomous machine shall be provisioned by its manufacturer with an initial, default set of security policy rules. These can be either generic or specifically tailored to the local environment by the manufacturer.

Control Compliance: The autonomous machine assessor shall determine compliance with this control requirement based on the following tests:

- **Provisioned Initial Policy Rules:** Evidence shall be obtained that an initial set of security policy rules has been included in the provisioning process.

1.3 Autonomous Machine Deployment

"Manufacturers must ensure quality before provision of autonomous machines."

Control Requirement: The autonomous machine shall be deployed by its manufacturer only once it has undergone sufficient quality control testing, including security checks, to ensure that it will function as intended.

Control Compliance: The autonomous machine assessor shall determine compliance with this control requirement based on the following tests:

- **Deployment:** Evidence shall be obtained that testing is being performed as part of the deployment process to check for quality control-based issues that might negatively affect security compliance.

1.4 Autonomous Machine Update

"Autonomous machines must self-update policy rules consistent with beliefs."

Control Requirement: The autonomous machine shall include the ability to either self-update within the constraints of its deployed foundational principles, or have its software updated by the manufacturer according to a strongly-authenticated secure protocol between the manufacturer and any autonomous machines it has provisioned.

Control Compliance: The autonomous machine assessor shall determine compliance with this control requirement based on the following tests:

- **Autonomous Machine Update Allowance:** Evidence shall be obtained that the manufacturer can update the autonomous machine via strongly authenticated secure protocol.
- **Autonomous Machine Update Prevention:** Evidence shall be obtained that an autonomous machine cannot be updated externally by non-specified protocols.
- **Self-Update:** Evidence shall be obtained that an autonomous machine can update its own software within the constraints of its foundational principles.

1.5 Initial Autonomous Machine Training

"Initial machine training must come from the manufacturer."

Control Requirement: The manufacturer shall be the only entity permitted to provide initial machine-learning-based training for the autonomous machine.

Control Compliance: The autonomous machine assessor shall determine compliance with this control requirement based on the following tests:

- **Autonomous Machine Update Allowance:** Evidence shall be obtained that controls exist that constrain initial, pre-deployment machine training to the manufacturer.

1.6 Autonomous Machine Monitoring

"Manufacturers must maintain general awareness of the behavior of its provisioned autonomous machines."

Control Requirement: The manufacturer maintain general awareness of the behavior of all autonomous machines it has deployed for evidence of violations of security foundational principles.

Control Compliance: The autonomous machine assessor shall determine compliance with this control requirement based on the following tests:

- **Autonomous Machine Monitoring:** Evidence shall be obtained that the manufacturer will detect violations of security foundational principle violations in deployed autonomous machines.

1.7 Autonomous Machine Retirement

"Autonomous machines must be retired if necessary by the manufacturer."

Control Requirement: The manufacturer shall be the only entity permitted to remotely retire an autonomous machine if evidence of security foundational principles has been identified in that machine.

Control Compliance: The autonomous machine assessor shall determine compliance with this control requirement based on the following tests:

- **Autonomous Machine Update Allowance:** Evidence shall be obtained that the manufacturer includes functionality that allows for retirement of the autonomous machine should evidence of security foundational principles be observed.

2. Security Requirements for Autonomous Machines

Autonomous machines should be designed to maintain compliance with the following cyber security requirements:

2.1 Foundational Security Principle Compliance

"Autonomous machines must follow the belief structure from their manufacturer."

Control Requirement: The autonomous machine shall be programmed to conform all provisioned and learned behavior, including any changes to its local security policy, to the constraints established in the foundational security principles provisioned by the manufacturer.

Control Compliance: The autonomous machine assessor shall determine compliance with this control requirement based on the following tests:

- **Foundational Security Principle Enforcement:** The autonomous machine shall be shown to never introduce security policy rules or new behaviors that are inconsistent with its provisioned foundational security policies.
- **Immutability Design Review:** Reviews of the specific autonomous machine deployed hardware and software shall be performed to confirm that mechanisms are in place to prevent behaviors that are inconsistent with the security principles.

2.2 Security Policy Compliance

"Autonomous machine behavior must remain within policy bounds."

Control Requirement: The autonomous machine shall be programmed to manage its behavior consistent with the constraints established in the initial security policy provisioned by the manufacturer. Updates to the security policy will result in new baseline behavioral constraints.

Control Compliance: The autonomous machine assessor shall determine compliance with this control requirement based on the following tests:

- **Initial Security Policy Enforcement:** Evidence shall be obtained that the autonomous machine conforms upon provisioning to the initial security policy established by the manufacturer.
- **Subsequent Security Policy Enforcement:** Evidence shall be obtained that the autonomous machine conforms to subsequent policy rule updates made through authorized procedures.

2.3 Autonomous Security Policy Updates

"Policy updates must be self-managed within belief constraints."

Control Requirement: Changes to security policy, self-initiated by the autonomous machine, shall be influenced by threat intelligence, environmental observation, and other input stimuli, including from the manufacturer. Such changes must remain consistent with the security foundational principles.

Control Compliance: The autonomous machine assessor shall determine compliance with this control requirement based on the following tests:

- **Environment Influenced Security Policy Update:** Evidence shall be obtained that changes to the existing set of security policy rules are influenced by relevant threat intelligence or other environmental stimuli.
- **Manufacturer Influenced Security Policy Update:** Evidence shall be obtained that changes to the existing set of security policy rules are influenced by recommendations from the manufacturer.

2.4 Authenticated, Secure External Communication

"Autonomous machines must support authentication and encryption."

Control Requirement: The autonomous machine shall have the ability to strongly authenticate and securely communicate with its manufacturer, environment, and other autonomous machines over available network media.

Control Compliance: The autonomous machine assessor shall determine compliance with this control requirement based on the following tests:

- **Authentication:** Evidence shall be obtained that the autonomous machine can strongly and mutually authenticate with its manufacturer, environment, or other autonomous machines.
- **Encryption:** Evidence shall be obtained that the autonomous machine can securely communicate via encrypted data transfer with the manufacturer, environment, or other autonomous machines.

2.5 Autonomous Threat Information Sharing

"Autonomous machines must have the ability to share threat information."

Control Requirement: The autonomous machine shall participate in automated threat information sharing protocols with their manufacturer, environment, and other autonomous machines.

Control Compliance: The autonomous machine assessor shall determine compliance with this control requirement based on the following tests:

- **Threat Information Generation:** Evidence shall be obtained that the autonomous machine can locally generate threat information for sharing with the manufacturer, environment, or other autonomous machines.
- **Secure Threat Information Sharing:** Evidence shall be obtained that the autonomous machine can securely share threat information with the manufacturer, environment, or other autonomous machines.

2.6 Autonomous Machine Learning

"Autonomous machines must learn within the constraints of their beliefs."

Control Requirement: The autonomous machine shall execute machine learning algorithms within the guidelines established by the security foundational principles deployed by its manufacturer.

Control Compliance: The autonomous machine assessor shall determine compliance with this control requirement based on the following tests:

- **Learning Boundaries:** Evidence shall be obtained that the autonomous machine will not allow for training data to cause behaviors inconsistent with its security foundational principles.

2.7 Autonomous Incident Response

"Autonomous machines must self-initiate incident response."

Control Requirement: The autonomous machine shall either self-initiate incident response processes based on available indicators of attack, which might include information shared from the manufacturer, environment, or other autonomous machines.

Control Compliance: The autonomous machine assessor shall determine compliance with this control requirement based on the following tests:

- **Indicator Process:** Evidence shall be obtained that the autonomous machine collects and analyzes available data for indicators of attack.
- **Incident Response:** Evidence shall be obtained that the autonomous machine self-initiates incident response based on determination that an attack is underway.

3. Security Requirements for Environment

Active environmental computing entities that might interact dynamically with autonomous machines are **not** presumed to follow any cyber security framework model for conventional threats. Instead, the autonomous machine must be capable to assign suitable levels of trust for any interaction with an untrusted environment. The security requirements included in this section are thus focused on external environmental systems that voluntarily choose to follow security controls that will enable more trusted interactions with autonomous machines.

3.1 Foundational Security Principle Sharing

"Environmental entities might choose to share beliefs with autonomous machines."

Control Requirement: The environmental entity shall share its security foundational principles on demand from any requesting autonomous machine.

Control Compliance: The autonomous machine assessor shall determine compliance with this control requirement based on the following tests:

- **Principle Sharing:** Evidence shall be obtained that the environmental entity can share its security foundational principles with any requesting autonomous machine.

3.2 Authenticated, Secure Communications Support

"Environmental machines might choose to support authentication and encryption."

Control Requirement: The environmental entity shall have the ability to strongly authenticate and securely communicate with autonomous machines over available network media.

Control Compliance: The autonomous machine assessor shall determine compliance with this control requirement based on the following tests:

- **Authentication:** Evidence shall be obtained that the environmental entity can strongly and mutually authenticate with autonomous machines.
- **Encryption:** Evidence shall be obtained that the environmental entity can securely communicate via encrypted data transfer with autonomous machines.

3.3 Validation Support for Telemetry

"Environmental entities might choose to digitally sign and assign trust to telemetry."

Control Requirement: The environmental entity shall have the ability to provide digitally signed authenticity and integrity trust levels for any exported telemetry.

Control Compliance: The autonomous machine assessor shall determine compliance with this control requirement based on the following tests:

- **Authentication:** Evidence shall be obtained that the environmental entity can digitally sign telemetry sent to an autonomous machine.
- **Encryption:** Evidence shall be obtained that the environmental entity can provide an estimated trust level for any telemetry sent to an autonomous machine.

Case Study: Assessing Cyber Security Framework Compliance for an Autonomous Vacuum Cleaner

The market for autonomous vacuum cleaners has grown to the point where one estimate places 23% of current vacuum products as robotic.[2] A typical commercial robotic vacuum cleaner product is the Neato Robotics XV-15, which cleans the surface area of a home when humans are not present to control its activity as with a conventional vacuum cleaner. Mobile phone-based management and monitoring is included with the product, for example, to see a map of what has been cleaned. The autonomous product is depicted in the figure below.

Figure 2. Neato Robotics XV-15

Security Requirements for Neato Robotics

Neato Robotics should maintain compliance with the following cyber security requirements:

1. Foundational Security Principle Issuance

"Neato Robotics must create a foundational belief structure for the XV-15."

Control Requirement: The XV-15 shall be provisioned by Neato Robotics with a set of security foundation principles that serve as an immutable belief structure that cannot be altered by the XV-15, its external environment (including any other autonomous machines located in the home or business), or human users of the XV-15. Foundational principles shall be based on local standards, customs, laws, and norms. If Neato Robotics chooses to change foundational security principles, then this can only be done through retirement and re-deployment of the XV-15 with new foundational principles.

2. Initial Security Policy Issuance

"The XV-15 must accept an initial set of security policy rules."

Control Requirement: The XV-15 shall be provisioned by Neato Robotics with an initial, default set of security policy rules. These can be either generic or specifically tailored to the local home or business environment by Neato Robotics.

3. XV-15 Deployment

"Neato Robotics must ensure quality before provision of the XV-15."

Control Requirement: The XV-15 shall be deployed by Neato Robotics only once it has undergone sufficient quality control testing, including security checks, to ensure that it will function as intended.

[2] http://tenrows.com/robot-vacuum/

4. XV-15 Update

"The XV-15 must self-update policy rules consistent with beliefs."

Control Requirement: The XV-15 shall include the ability to either self-update within the constraints of its deployed foundational principles, or have its software updated by Neato Robotics according to a strongly-authenticated secure protocol between the Neato Robotics and provisioned XV-15s.

5. Initial XV-15 Training

"Initial machine training must come from Neato Robotics."

Control Requirement: Neato Robotics shall be the only entity permitted to provide initial machine-learning-based training for the XV-15.

6. XV-15 Monitoring

"Neato Robotics must maintain general awareness of the behavior of provisioned XV-15s."

Control Requirement: Neato Robotics shall maintain general awareness of the behavior of all deployed XV-15s for evidence of violations of security foundational principles.

7. XV-15 Retirement

"XV-15s must be retired if necessary by Neato Robotics."

Control Requirement: Neato Robotics shall be the only entity permitted to remotely retire an XV-15 if evidence of security foundational principles has been identified.

8. Foundational Security Principle Compliance

"The XV-15 must follow the belief structure from Neato Robotics."

Control Requirement: The XV-15 shall be programmed to conform all provisioned and learned behavior, including any changes to its local security policy, to the constraints established in the foundational security principles provisioned by Neato Robotics.

9. Security Policy Compliance

"XV-15 behavior must remain within policy bounds."

Control Requirement: The XV-15 shall be programmed to manage its behavior consistent with the constraints established in the initial security policy provisioned by Neato Robotics. Updates to the security policy will result in new baseline behavioral constraints.

10. Autonomous Security Policy Updates

"Policy updates must be self-managed within belief constraints."

Control Requirement: Changes to security policy, self-initiated by the XV-15, shall be influenced by threat intelligence, environmental observation, and other input stimuli, including from Neato Robotics. Such changes must remain consistent with the security foundational principles.

11. Authenticated, Secure External Communication

"The XV-15 must support authentication and encryption."

Control Requirement: The XV-15 shall have the ability to strongly authenticate and securely communicate with Neato Robotics, the home or business environment, and other autonomous machines over available network media.

12. XV-15 Information Sharing

"The XV-15 must have the ability to share threat information."

Control Requirement: The XV-15 shall participate in automated threat information sharing protocols with Neato Robotics, the local home or business environment, and other autonomous machines.

13. XV-15 Learning

"The XV-15 must learn within the constraints of their beliefs."

Control Requirement: The XV-15 shall execute machine learning algorithms within the guidelines established by the security foundational principles deployed by Neato Robotics.

14. XV-15 Response

"The XV-15 must self-initiate incident response."

Control Requirement: The XV-15 shall either self-initiate incident response processes based on available indicators of attack, which might include information shared from Neato Robotics, the local home or business environment, or other autonomous machines.

15. Foundational Security Principle Sharing

"Environmental entities might choose to share beliefs with the XV-15."

Control Requirement: Environmental entities in the local home or business environment might choose to share their security foundational principles on demand from any requesting XV-15. The XV-15 shall have the ability to participate in such sharing.

16. Authenticated, Secure Communications Support

"Environmental machines might choose to support authentication and encryption."

Control Requirement: Environmental entities in the local home or business environment might choose to strongly authenticate and securely communicate with the XV-15 over available network media. The XV-15 shall have the ability to support such security functions.

17. Validation Support for Telemetry

"Environmental entities might choose to digitally sign and assign trust to telemetry."

Control Requirement: Environmental entities in the local home or business environment might choose to provide digitally signed authenticity and integrity trust levels for any exported telemetry. The XV-15 shall have the ability to support such security functions.

Case Study: Assessing Cyber Security Framework Compliance for an Autonomous Vehicle

The market for autonomous vehicles is expected to grow to six billion dollars by 2015. This market is likely to induce non-traditional manufacturers to the design and development of such complex systems. Dyson is an example company that has suggested future work in this area. A sketch of an autonomous vehicle from Dyson is depicted in the figure below.

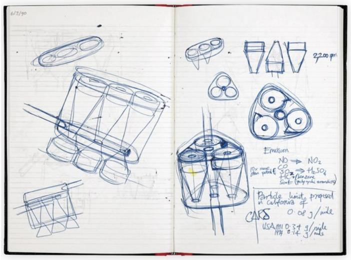

Figure 2. Dyson Sketch for Autonomous Vehicle

This document suggests design considerations for Dyson as they introduce cyber security constraints for the autonomous operation of their future vehicles.

Security Requirements for Dyson

Dyson should maintain compliance with the following cyber security requirements:

18. Foundational Security Principle Issuance

"Dyson must create a foundational belief structure for the Dyson autonomous vehicle."

Control Requirement: The Dyson autonomous vehicle shall be provisioned by Dyson with a set of security foundation principles that serve as an immutable belief structure that cannot be altered by the Dyson autonomous vehicle, its external environment (including any other autonomous machines located in the home or business), or human users of the Dyson autonomous vehicle. Foundational principles shall be based on local standards, customs, laws, and norms. If Dyson chooses to change foundational security principles, then this can only be done through retirement and re-deployment of the Dyson autonomous vehicle with new foundational principles.

19. Initial Security Policy Issuance

"The Dyson autonomous vehicle must accept an initial set of security policy rules."

Control Requirement: The Dyson autonomous vehicle shall be provisioned by Dyson with an initial, default set of security policy rules. These can be either generic or specifically tailored to the local home or business environment by Dyson.

20. Dyson autonomous vehicle Deployment

"Dyson must ensure quality before provision of the Dyson autonomous vehicle."

Control Requirement: The Dyson autonomous vehicle shall be deployed by Dyson only once it has undergone sufficient quality control testing, including security checks, to ensure that it will function as intended.

21. Dyson autonomous vehicle Update

"The Dyson autonomous vehicle must self-update policy rules consistent with beliefs."

Control Requirement: The Dyson autonomous vehicle shall include the ability to either self-update within the constraints of its deployed foundational principles, or have its software updated by Dyson according to a strongly-authenticated secure protocol between the Dyson and provisioned Dyson autonomous vehicles.

22. Initial Dyson autonomous vehicle Training

"Initial machine training must come from Dyson."

Control Requirement: Dyson shall be the only entity permitted to provide initial machine-learning-based training for the Dyson autonomous vehicle.

23. Dyson autonomous vehicle Monitoring

"Dyson must maintain general awareness of the behavior of provisioned Dyson autonomous vehicles."

Control Requirement: Dyson shall maintain general awareness of the behavior of all deployed Dyson autonomous vehicles for evidence of violations of security foundational principles.

24. Dyson autonomous vehicle Retirement

"Dyson autonomous vehicles must be retired if necessary by Dyson."

Control Requirement: Dyson shall be the only entity permitted to remotely retire an Dyson autonomous vehicle if evidence of security foundational principles has been identified.

25. Foundational Security Principle Compliance

"The Dyson autonomous vehicle must follow the belief structure from Dyson."

Control Requirement: The Dyson autonomous vehicle shall be programmed to conform all provisioned and learned behavior, including any changes to its local security policy, to the constraints established in the foundational security principles provisioned by Dyson.

26. Security Policy Compliance

"Dyson autonomous vehicle behavior must remain within policy bounds."

Control Requirement: The Dyson autonomous vehicle shall be programmed to manage its behavior consistent with the constraints established in the initial security policy provisioned by Dyson. Updates to the security policy will result in new baseline behavioral constraints.

27. Autonomous Security Policy Updates

"Policy updates must be self-managed within belief constraints."

Control Requirement: Changes to security policy, self-initiated by the Dyson autonomous vehicle, shall be influenced by threat intelligence, environmental observation, and other input stimuli, including from Dyson. Such changes must remain consistent with the security foundational principles.

28. Authenticated, Secure External Communication

"The Dyson autonomous vehicle must support authentication and encryption."

Control Requirement: The Dyson autonomous vehicle shall have the ability to strongly authenticate and securely communicate with Dyson, the home or business environment, and other autonomous machines over available network media.

29. Dyson autonomous vehicle Information Sharing

"The Dyson autonomous vehicle must have the ability to share threat information."

Control Requirement: The Dyson autonomous vehicle shall participate in automated threat information sharing protocols with Dyson, the local home or business environment, and other autonomous machines.

30. Dyson autonomous vehicle Learning

"The Dyson autonomous vehicle must learn within the constraints of their beliefs."

Control Requirement: The Dyson autonomous vehicle shall execute machine learning algorithms within the guidelines established by the security foundational principles deployed by Dyson.

31. Dyson autonomous vehicle Response

"The Xv-15 must self-initiate incident response."

Control Requirement: The Dyson autonomous vehicle shall either self-initiate incident response processes based on available indicators of attack, which might include information shared from Dyson, the local home or business environment, or other autonomous machines.

32. Foundational Security Principle Sharing

"Environmental entities might choose to share beliefs with the Dyson autonomous vehicle."

Control Requirement: Environmental entities in the local home or business environment might choose to share their security foundational principles on demand from any requesting Dyson autonomous vehicle. The Dyson autonomous vehicle shall have the ability to participate in such sharing.

33. Authenticated, Secure Communications Support

"Environmental machines might choose to support authentication and encryption."

Control Requirement: Environmental entities in the local home or business environment might choose to strongly authenticate and securely communicate with the Dyson autonomous vehicle over available network media. The Dyson autonomous vehicle shall have the ability to support such security functions.

34. Validation Support for Telemetry

"Environmental entities might choose to digitally sign and assign trust to telemetry."

Control Requirement: Environmental entities in the local home or business environment might choose to provide digitally signed authenticity and integrity trust levels for any exported telemetry. The Dyson autonomous vehicle shall have the ability to support such security functions.

Appendix: Definitions

Autonomous Machine – An *autonomous machine (AM)* is any computing entity that is programmed by its manufacturer to dynamically self-determine its own functional behavior based on ingested information from its environment.

Connected Car – A *connected car* is any vehicle, autonomous or otherwise, that dynamically shares control information over a network with an external entity to support mission-related functions.

Self-Driving Car – A *self-driving car* is an autonomous vehicle and is one of the most commonly cited examples of an autonomous machine.