Product Cybersecurity Policy

Purpose

Allison Transmission, Inc. ("Allison") is committed to protecting against potential vulnerabilities that could affect the integrity and security of our products and systems. The threat of cyberattacks or unauthorized electronic access or control to wireless connected products is constantly evolving. In response, we have proactively established a coordinated product cybersecurity management and oversight framework that is focused on reducing the cybersecurity risks from new and emerging threats, enabling us to continuously improve the security of our products.

Allison recognizes the importance of incorporating cybersecurity considerations throughout the product development process. Allison is also committed to ensuring that all personnel involved in the product development process understands that cybersecurity is paramount in protecting Allison products and digitally connected services. It is important that Allison implements and maintains reasonable security safeguards to protect the security of vehicle electronics from interruptions to the intended use of the propulsion system, and from vulnerabilities that could result in the interruption of the intended mission of a vehicle.

This Product Cybersecurity Policy ("Policy") describes high level direction for product cybersecurity management and oversight to mitigate against cybersecurity threats.

Scope

The scope of this Policy includes all applications equipped with Allison's 6th Generation transmission control module and digitally connected services that are developed, implemented, or maintained by Allison.

Additionally, this Policy applies to all Allison personnel involved in the development, implementation, and maintenance of vehicle products and digitally connected services deployed by Allison, especially those involved with Vehicle Electronic Programming Station systems and managing third party contracts that impact, in whole or in part, digitally connected services and products.

Principles, Policies, and Practices

As a guide to securing products, Allison's policies align with the following principles:

1. Holistic Approach. It is imperative that all stakeholders and Allison personnel collaborate to take a thoughtful, holistic approach to securing all phases of applicable vehicle products and digitally connected services development and implementation processes. An inclusive process must focus on end-to-end security, including security-by-design techniques and secure development lifecycles. Security by design shall be considered throughout the lifecycle of the vehicle and digitally connected services. Allison's product cybersecurity management and oversight framework must be developed to identify, prevent, investigate, and mitigate cybersecurity vulnerabilities and perform any required recovery actions to remedy the impact. Additionally, Allison products and digitally connected services shall be developed in accordance with principles of secure software development consistent with software development industry best practices.

This Policy further supports Allison's overarching cybersecurity goals of mitigating cyber security threats through the use of state of the art electronic hardware and software security functions, minimizing the impact to existing workflows in engineering, manufacturing, quality, customer support and Information Technology, and to minimize the impact to customers and end users.

2. Industry-Driven Core Baselines and Standards. Allison must lead with industry-driven core baselines and standards for security capabilities. Assisting in the development and implementation of a common set of best practices and secure capabilities that are broadly applicable across the vehicle product and digitally connected services industry with varying levels of complexity and are driven by market demand will help to improve the industry's cybersecurity.

3. Continuous Adaptation. Allison understands that vehicle products and digitally connected services is a long-term commitment, not a one-time design and manufacturing cost. Product cybersecurity demands dynamic, flexible, market-driven solutions that are nimble and adaptable to evolving cyber threats, including those specific to the proliferation of vehicle products and digitally connected services. As baseline security requirements through the development and the lifecycle of Allison products, Allison shall implement processes to ensure malware protection measures are implemented for the products development environment and relevant assets and maintain processes to ensure the systems used in products development environment(s) are properly and timely patched.

Deviations from this Policy must be considered and approved in accordance with Allison's risk assessment policy and procedure.

Allison understands that a robust cyber security strategy for heavy duty vehicle & related applications has implications outside of Allison direct controls, including our suppliers, customers, and distribution channel. Development, integration, etc. done by OEMs should support this policy and support robust product cyber security at a vehicle & end user level.

Compliance Monitoring

Allison, channel and supplier personnel engaged in work that directly or indirectly affects any vehicle products or digitally connected services deployed by Allison must be able to include industry best practices and design in compliance with this Policy.

Allison shall choose methods in accordance with applicable standards, regulations, risk assessment objectives, culture, and available resources to assess compliance with this Policy.

This Policy documents Allison's intent to ensure the security of Allison products and digitally connected services. However, Allison also recognizes that OEMs may not accept the implemented standards, practices, guidelines and controls aimed at securing Allison products from unauthorized electronic access and control as optimized for their applications. Accordingly, deviations from this Policy must be considered and approved in accordance with Allison's risk assessment policy and procedure.

Related Documents

This Policy serves as a high level directive that is part of the overall management of the product cybersecurity management and oversight framework. No single document can cover all the possible cybersecurity issues that Allison may face, therefore, Allison personnel must refer to related documents to include applicable standard operating procedures, specifications, protocols and practices relating to the development and implementation of vehicle products and digitally connected services.

This policy is consistent with and supported by Allison's Written Information Security Program ("WISP").

Cybersecurity Incident Response Team

Allison's Product Cybersecurity Incident Response Team is responsible for responding, containing, and fixing the reported(identified) incidents(vulnerability) affecting Allison Products. Our team consists of experienced members from cross-functional organizations across Allison. The team regularly reviews our policies, and gets trained on new regulations/industry standards as required.

Effective Date: May 24, 2021