SECTION 25:

Product Cybersecurity

A. SUMMARY

This Carrier Product Cybersecurity Policy documents and provides clarification and instruction on a variety of key practices and activities that enable Product and Service development teams to deliver safe, reliable, and competitive Products and Services in a cybersecure manner.

B. APPLICABILITY

This Policy applies to Carrier and any Product or Service, as defined in Exhibit 1.

Carrier will undertake to have its Service Providers comply with this Policy or equivalent requirements in the conduct of their business with Carrier through appropriate contractual requirements.

Local laws, regulations, and other restrictions applicable to Carrier or any Operating Business shall be applied to the extent of a conflict with this Policy.

The Carrier VP, Chief Information Security Officer (CISO) and the CTO, SVP of Global Engineering (CTO) are the executive co-sponsors of this policy and designate the Carrier Chief Product Security Officer (CPSO) as owner, responsible to maintain, fulfill and enforce the provisions herein.

Any deviation from this Policy must be approved in writing by the Carrier CPSO (or designee) prior to implementation.

C. DEFINITIONS

Exhibit 1 provides definitions for terms used in this Policy.

All capitalized terms not defined in this Policy (including Exhibit 1) are defined in CPM 1: Governance and Definitions including Exhibit 1: Compliance Glossary.

D. PRINCIPLES

Carrier will endeavor to adhere to the following Product Cybersecurity principles in every Product or Service development, introduction, deployment, support and/or maintenance activity:

1. Application of the Carrier Way is a fundamental requirement for secure product development and lifecycle support.

2. Cybersecurity is everyone's business and Product Cybersecurity is a team sport that requires situational awareness, domain expertise, context, collaboration, transparency and continual analysis, improvement, and vigilance.

3. Application and implementation of the appropriate proactive and reactive security controls is a necessity throughout all phases of the Secure Product Development and Support Lifecycle, in accordance with industry standards and best practices for cybersecurity, and in a manner that ensures Carrier and customer mission success.

4. Comprehensive identification and proactive management of all cybersecurity risk in an independently auditable manner is foundational to support the Carrier standard for security maturity.

5. The highest standards shall be pursued in building and continually improving capabilities, practices, and activities in the cybersecurity domain areas of secure deployment, threat intelligence, monitoring, and cybersecurity incident response, to consistently provide responsible cybersecurity channel and customer support, and transparency for post-development operational excellence.

6. Processes, Products, Services, and outcomes shall aim to align with and, where possible, exceed appropriate industry best practices, and codes and standards, in a manner that transcends fundamental security maturity norms and innovates such that cybersecurity differentiates the Carrier brand, offerings and Operating Businesses.

E. POLICY

1. **Compliance with Law:** At a minimum, Carrier will comply with all laws and regulations relating to Cybersecurity applicable to its Operating Businesses worldwide.

2. **General**: The CPSO (or designee) shall act as governing authority relating to all matters of Product or Service cybersecurity at Carrier, including but not limited to secure development, post-development product cybersecurity operations, cybersecurity commercial innovation, and monetizing cybersecurity. When and where possible and as necessary, the CPSO (or designee) shall endeavor to work collaboratively with any related/relevant Product Cybersecurity stakeholder(s) to ensure, maintain and support continuity, context, and universal mission success for Carrier and its customers.

3. **Carrier Product Cybersecurity Council (PCC)**: The Product Cybersecurity Council will be convened as needed and as determined by the CPSO to hear appropriate requests, critical policy exceptions, escalations, risk acceptance/transference, and matters requiring high-level executive visibility and attention. The CISO and the CTO will Co-Chair the PCC, with the CPSO serving as moderator. Other members of the PCC will be comprised of leadership stakeholders from Carrier, as needed and dependent upon context of the issues/requests at hand, in accordance with Global Product Cybersecurity standard operating procedure. Tactical and operational stakeholders will attend and present to the Council as necessary to support new requests and engagements. The decision of the PCC will be considered final in escalations, issues and disputes presented for consideration.

4. **Codes and Standards**: Carrier shall comply with appropriate industry codes and standards to ensure competitive advantage and regulatory compliance in the domain of cybersecurity. It is the responsibility of the CPSO (or designee) to establish standards-based strategy(s), identify relevant list(s) of codes and standards (where applicable) to meet mission requirements, and/or work instructions applicable to Carrier Product(s) and Service(s) for the cybersecurity discipline.

5. **Product Cybersecurity Standards**: Product Cybersecurity standard work documents, standards, process(es) and/or workflows shall be established by the CPSO (or designee). These documents shall enable and govern the Carrier Secure Product Development & Support Lifecycle (SPDL), including but not limited to the necessary cybersecurity controls, requirements, architecture, analysis, testing and risk management practices and activities to provide for acceptable risk tolerances, consistent and auditable standard work and outcomes, compliance with strategic standards, post-deployment support, and optimal results to assure mission success and Carrier brand defense. Product Cybersecurity standard work documents and standards shall be updated at intervals, as defined by the CPSO (or designee).

6. **Risk Management**: Appropriate designee(s) responsible for Carrier Products and Services shall collaborate with the CPSO (or designee) to identify, manage, and mitigate cybersecurity risks, defects and/or issues associated with Product or Service design, development, maintenance, and support, using a Carrier-common methodology, as defined in Product Cybersecurity standard work documents and standards. Relevant stakeholders, constraints, system components, materials, integrations, and technologies shall be identified and documented, with appropriate cybersecurity controls applied in accordance with Product Cybersecurity standards. Product cybersecurity risks shall be scored leveraging a suitable and standard methodology, and are managed in accordance with established tolerance levels, as defined in Product Cybersecurity standards. The Carrier Product Cybersecurity Council (PCC) will be convened on a periodic basis (as needed), as determined by the CPSO, to hear appropriate escalations and requests for risk escalation, acceptance, transference, and management.

7. **Governance**: Unless deemed out-of-scope for cybersecurity controls by Global Product Cybersecurity (GPC), Product and Service changes, maintenance, support and new development shall be governed consistently across Carrier, in accordance with appropriate industry standards, with practices and activities that shall be auditable and shall include suitable context-based cybersecurity controls, requirements, architecture, analysis and testing, with risk management practices and activities applied to provide for acceptable risk tolerances and optimal results and outcomes to assure mission success and Carrier brand defense, as prescribed in Product Cybersecurity standard work documents and standards and/or as deemed necessary by the CPSO. Independent gating and/or release approval shall be provided by GPC and is required prior to Product or Service phase gate transition and/or deployment/release, in accordance with Carrier Product Development Process (PDP) policies, standards and guidelines and with GPC standard work documents and standards. Production disputes and escalations shall be resolved by the CPSO (or designee), within PDP Boards (PRBs), or when necessary, within a PCC engagement, in accordance with GPC standard operating procedure.

8. **Cybersecurity Tooling**: Cybersecurity tooling shall be standardized, consolidated, and centrally managed and governed by Carrier Global Product Cybersecurity (GPC) to ensure consistent execution and outcomes, clear and transparent risk identification and management, assure standards-based compliance, and enable economies of scale. Products and Services at Carrier shall leverage a common, centrally managed GPC cybersecurity toolset, at the direction of the CPSO (or designee) in accordance with Product Cybersecurity standards, and in a manner that ensures customer and Carrier mission success.

9. **Cybersecurity Testing**: Cybersecurity testing (such as penetration testing, compliance testing, and validation testing) shall be air-gapped from development and an objectively independent, standardized, centralized, consolidated team function under the direction of GPC, and shall align to industry best practices. Cybersecurity testing shall be maintained, managed, and executed by Global Product Cybersecurity (GPC). Products and Services at Carrier shall undergo, at regular appropriate intervals, professional and standards-compliant cybersecurity testing, both internally and externally as deemed necessary, in accordance with GPC standards, and in a manner that ensures customer and Carrier mission success.

10. **Deliverables**: Cybersecurity deliverables, including all designated security artifacts, shall be collected throughout all designated phases of the Secure Product Development & Support Lifecycle (SPDL). Cybersecurity deliverables shall be made available to all relevant stakeholders and retained and secured per Carrier's record retention polices and in accordance with Product Cybersecurity standard work documents and standards. This ensures proper controls for backup and protection against loss, as well as enablement of audit, continual analysis, and product cybersecurity maturity improvement.

11. **Enforcement**: Carrier will enforce this Policy and the procedures issued to implement it. Failure to adhere to this Policy or the procedures implementing it may lead

to disciplinary action for employees. Carrier will establish clear, fair, and consistent disciplinary procedures across the enterprise.

F. ROLES AND RESPONSIBILITIES

1. **Chief Information Security Officer (CISO)** is the co-executive sponsor of this policy. CISO shall coordinate with the CTO to designate global responsibility to (1) execute the duties of the Carrier Global Product Cybersecurity mission(s), (2) manage and maintain this Policy and supporting standard work documents and standards, and (3) ensure Carrier and customer mission success for Product Cybersecurity.

2. **Chief Technology Officer, SVP of Global Engineering (CTO)** is the co-executive sponsor of this policy. CISO shall coordinate with the CTO to designate global responsibility to (1) execute the duties of the Carrier Global Product Cybersecurity mission(s), (2) manage and maintain this Policy and supporting standard work documents and standards, and (3) ensure Carrier and customer mission success for Product Cybersecurity.

3. **Chief Product Security Officer (CPSO)** shall be the owner of this policy, and the primary global designee responsible for maintaining, monitoring, and improving, as needed, reasonable and appropriate technical and administrative safeguards, capabilities, and controls to protect the security posture of Carrier Products and Services, ensure the cybersecurity related competitive advantages of Carrier, and enable post-deployment cybersecurity support of Carrier Products and Services. CPSO shall ensure that the Carrier Global Product Cybersecurity (GPC) Program is strategically and tactically able to meet the operational and compliance requirements of this Policy and supporting standards and shall endeavor to drive Carrier and customer mission success in all phases of the Secure Product Development & Support Lifecycle (SPDL). CPSO shall ensure that the Carrier Product Cybersecurity Council (PCC) is informed with respect to critical cybersecurity requests, policy exceptions, escalations, and risk acceptance/transference. CPSO shall ensure that Product Cybersecurity process(es), procedures, practices, and activities are consistent, repeatable, auditable, effective, and continually improving at Carrier.

4. **Product Cybersecurity Officer(s) (PCOs)** report to the Carrier CPSO and will support all facets of the Carrier Global Product Cybersecurity (GPC) Program, as needed. Various types of PCOs may be designated by a CPSO including, among others, a Deputy CPSO (D-CPSO), Regional PCOs (RPCOs), and Business Unit PCOs (BPCOs). PCOs shall assist the Carrier CPSO within various focus areas and shall manage varying levels of responsibility to enable operational excellence and ensure strategic and tactical outcomes for the Global Product Cybersecurity mission(s). PCOs will ensure that Product Cybersecurity process(es), procedures, practices, and activities are executed in accordance with this Policy and supporting standard work documents and standards in a manner that ensures customer and Carrier mission success.

5. **Product Cybersecurity Mission Leader(s) (MLs)** report to the Carrier CPSO and will strategically and tactically lead one of three major missions of the Carrier Global Product Cybersecurity (GPC) Program. Those missions are: (1) Secure Product Development, (2) Post-Development Product Cybersecurity Operations, and (3) Cybersecurity Commercial Innovation. The three major mission areas maintained across Carrier by GPC MLs are considered an interconnected and relational set which forms the complete Secure Product Development & Support Lifecycle (SPDL). MLs will be directly responsible to mutually govern Secure Development Lifecycle Assurance (SDLA), Post-Development Product Cybersecurity Operations (PCSO), and shall ensure cybersecurity as a driver of innovation, differentiation, and market/channel enablement. MLs (or designees) shall directly support Carrier product development and ensure that Product Cybersecurity process(es), procedures, practices, and activities are executed in accordance with this Policy and supporting standard work documents and standards in a manner that ensures customer and Carrier mission success.

6. **Cybersecurity Fellow(s) (CFs)** report to the CPSO and will strategically and tactically support Carrier, Global Product Cybersecurity (GPC), and one or more of the three GPC major missions. CFs will also dedicate a portion of their time to the mission objectives and activities of the Carrier Fellows Organization. CFs are recognized experts in the cybersecurity discipline both within the company and across the industry. They are focused on technical excellence, adaptability, innovation and driving strategic technologies for the company. While they are cybersecurity discipline specialists, they may also possess broad ranges of domain and technical expertise across the business and shall leverage that experience to drive engineering effectiveness and innovation. CFs also serve to transfer their knowledge through training, mentoring, and fostering best in class capabilities for Carrier.

7. **Product Cybersecurity Architect(s) (CAs)** report to the CPSO, D-CPSO or ML(s) and will tactically support one or more of three major missions of the Carrier Global Product Cybersecurity (GPC) Program. CAs shall work directly and collaboratively with Cybersecurity Champions, Product Managers and production teams focused on product development and engineering to ensure secure design, development, and support mission success. CAs shall work to ensure best outcomes for product cybersecurity stakeholders and will enable and empower Cybersecurity Champions to achieve compliance with Product Cybersecurity process(es), procedures, practices, and activities in accordance with this Policy and supporting standard work documents and standards in a manner that ensures customer and Carrier mission success. The Cybersecurity Architect – Cybersecurity Champion collaborative partnership is the fundamental bi-directional mentor-mentee enabler that makes possible standards-based secure development that scales, provides consistency, auditability, and ensures Product, Service and business-level domain expertise is maintained, while ensuring best outcomes for mission success for Carrier and all product cybersecurity stakeholders.

8. **Cybersecurity and Penetration Tester(s) (PTs)** report to the CPSO, D-CPSO or PSL(s) and will tactically support one or more of three major missions of the Carrier Global

Product Cybersecurity (GPC) Program. Cybersecurity and Penetration Testers at Carrier shall work collaboratively as members of a coordinated, consolidated, and professional cybersecurity testing team to achieve objective compliance with appropriate and designated cybersecurity standards and meet industry best practices for operational excellence by leveraging mutually beneficial diverse cyber-attack and red-teaming skillsets as well as crowd-sourcing strategies. PTs shall work under the professional direction of GPC cybersecurity testing domain experts to ensure best outcomes for product cybersecurity stakeholders and will enable Product and Service development teams to achieve compliance with Product Cybersecurity process(es), procedures, practices, and activities in accordance with this Policy and supporting standard work documents and standards, and in a manner that ensures customer and Carrier mission success.

9. **Cybersecurity Champion(s) (CCs)** is a part-time role and responsibility aligned to a single project – not necessarily a component, system, product, or business. The CC role shall be fulfilled by active developers associated with respective development projects, and selection of appropriate CCs shall be driven and dependent upon project context, domain knowledge and capability requirements. CC(s) shall be designated to support all (in-scope for cybersecurity) Product and Service development projects during project inception or at the start of planning and specification phases. CC(s) shall be direct role player(s) positioned to, and capable of, collaboratively (in partnership with a designated GPC Cybersecurity Architect) support Product Cybersecurity process(es), procedures, practices, and activities in accordance with this Policy and supporting standard work documents and standards in a manner that ensures customer and Carrier mission success. Cybersecurity Champion(s) may be nominated by Carrier product development team leaders or GPC Cybersecurity Architect(s) but must meet the approval requirements of GPC and must maintain and execute associated duties until conclusion of the subject project(s). CC(s) can be replaced or removed, at the discretion of GPC. The Cybersecurity Champion – Security Architect collaborative partnership is the fundamental bi-directional mentor-mentee enabler that makes possible standards-based secure development that scales, provides consistency, auditability, and ensures Product, Service and business-level domain expertise is maintained, while ensuring best outcomes for mission success for Carrier and all product cybersecurity stakeholders.

10. **BU Level Product Cybersecurity FTEs/Contributors (Non-GPC)** may optionally be employed by Carrier Business Units, Segments, Reporting Units, Sub-Reporting Units, and all worldwide divisions, operating businesses, and entities to help support the localized product cybersecurity mission demands, requirements, and operations. While BU Cyber FTE/contributor(s) shall report tactically and operationally to their own BU-level report chain, such individuals and their respective report chains must also operate in alignment, collaboratively, transparently, and in compliance with the strategy, operations, and mission objectives of GPC, the Carrier CPSO, and designees. All BU Cyber FTE/contributor(s) must comply with this Policy and all standard work documents, standards, process(es) and procedures issued to implement it. To ensure operational excellence, BU Cyber FTE/Contributors shall adhere to strategic direction and guidance

provided by GPC MLs. When and where possible and appropriate, GPC MLs shall endeavor to support BU Cyber FTE/Contributors to assist and ensure the unique needs of diverse business-level teams are met.

11. **Carrier Employees and Leased Labor** (e.g., onsite, or offsite contract workers) must comply with this Policy and all standard work documents, standards, process(es) and procedures issued to implement it. All employees and leased labor must safeguard the security posture of all Carrier Products and Services and shall work in close coordination with Global Product Cybersecurity (GPC) to support the three major GPC missions. All employees and leased labor must work transparently with GPC and report any known or suspected cybersecurity defects, risks, breaches, or incidents immediately and/or as prescribed within Product Cybersecurity standards.

G. REFERENCES

All referenced CPM and CPSW can be retrieved from ePolicy.

- CYB-SW-0 – Global Product Cybersecurity Secure Development Lifecycle (SDL)
- CYB-SW1 – (W1) Cyber Passport – Waterfall
- CYB-SW2 – (W2) Cyber Passport – Waterfall Lite
- CYB-SW3 – (A1) Agile Cyber – MVP & Next Release
- CYB-SW4 – (A2) Agile Cyber – Continuous Release
- CYB-S1 - Security Design Requirements Standard
- CYB-S2 - Threat Modeling Standard version
- CYB-S3 - Static Application Security Testing Standard
- CYB-S4 - Software Composition Analysis Standard
- CYB-S5 - Risk Scoring Standard
- CYB-S6 - Vulnerability management Standard
- CYB-S7 - Product Security Penetration Testing Standard
- CYB-S8 - Product Security Incident Response – PSIRT
- CYB-S9 - Coding Standards
- CYB-S10 - Threat Intelligence Standard
- CYB-S11 - Security Requirements Standard
- CYB-S12 - Product Cybersecurity Secure Deployment Documentation Standard
- CYB-S13 - Product Cybersecurity Change Management Standard
- CYB-S14 - Product Cybersecurity Configuration Management Standard