Product Cybersecurity Appendix

Guidelines

In the event that any Products (as defined below) supplied under the Agreement include executable binary code, Supplier agrees to comply with the requirements set forth in these Guidelines. In the event of any inconsistency or conflict between these Guidelines and any other provision of the Agreement with respect to a subject covered by these Guidelines, the provision requiring the more stringent requirement shall prevail. The requirements in these Guidelines are in addition to any cybersecurity-related obligations between GE and the Supplier under the Agreement.

Part A: Definitions

(i) "Copyleft License" means the GNU General Public Licenses version 2.0 (GPLv2) or version 3.0 (GPLv3), Affero General Public License version 3 (AGPLv3), or any other license that requires, as a condition of use, modification and/or distribution of or making available over a network any materials licensed under such a license to be: (a) licensed under its original license; (b) disclosed or distributed in source code form; (c) distributed at no charge; or (d) subject to restrictions on assertions of a licensor's or distributor's patents.

(ii) "Cybersecurity Vulnerability (ies)" means any bug, software defect, design flaw, or other issue with software associated with a Product that could adversely impact the confidentiality, integrity or availability of information or processes associated with the Product.

(iii) "Open Source Software" means any material that is distributed as "open source software" or "freeware" or is otherwise distributed publicly or made generally available in source code form under terms that permit modification and redistribution of the material on one or more of the following conditions: (a) that if the material, whether or not modified, is redistributed, that it shall be: (i) disclosed or distributed in source code form; (ii) licensed for the purpose of making derivative works; and/or (iii) distributed at no charge; (b) that redistribution must be licensed or distributed under any Copyleft License, or any of the following license agreements or distribution models: (1) GNU's General Public License (GPL), Lesser/Library GPL (LGPL), or Affero General Public License (AGPL), (2) the Artistic License (e.g., PERL), (3) the Mozilla Public License, (4) Common Public License, (5) the Sun Community Source License (SCSL), (6) the BSD License, (7) the Apache License and/or (8) other Open Source Software licenses; and/or (c) which is subject to any restrictions on assertions of patents.

(iv) "Product(s)" mean any goods, products, software and deliverables supplied under the Agreement.

(v) "Third Party Materials" means materials which are incorporated by Supplier in any Products provided to GE, the proprietary rights to which are owned by one or more third party individuals or entities.

Part B: Secure Software Development

1. Supplier shall ensure all Products have been developed in accordance with principles of secure software development consistent with software development industry best practices, including, security design review, secure coding practices, risk based testing and remediation requirements. Supplier's software development environment used to develop the Products must have security controls that can detect and prevent attacks by use of network layer firewalls and intrusion detection/prevention systems (IDS/IPS) in a risk based manner.

2. Supplier shall implement processes to ensure malware protection measures are implemented for the Products development environment and relevant assets.

3. The Supplier shall have a process to ensure the systems used in Products development environment(s) are properly and timely patched.

4. Supplier shall include cybersecurity guidance in the Product documentation provided to GE. This documentation shall include guidance on how to configure the Products and/or the surrounding environment to best ensure security. It shall also include guidance on which logical or physical ports are required for the product to function. If authentication is used to protect access to any service or capability of the Products, regardless of the intended user of that service/capability, the Supplier shall ensure:

    (i) the Products shall not provide access to that service or capability using a default account/password;
    (ii) the Products shall be configured with least privilege for all user accounts, file systems, and application-to-application communications, examples of file systems which implement file protection based on privileges are *nix and NTFS;
    (iii) the Products shall not provide access to that service or capability using a "Backdoor" account or password;
    (iv) the Products' associated authentication and password change processes shall be implemented with an appropriately secure cryptographic level; and
    (v) GE shall be able to change any passwords supported by the Products.

5. Services or capabilities that are not required to implement the Product's functionality shall by default be disabled, or shall require authentication to protect access to this service or capability.

6. In the event that any wireless technology is incorporated in any Product, Supplier shall document that the wireless technology complies with standard operational and security requirements specified in applicable wireless standard(s) or specification(s) (e.g., applicable IEEE standards, such as 802.11).

7. In the event that any cryptographic systems are contained in the Product, Supplier shall only use cryptographic algorithms and key lengths that meet or exceed the most current version of the National Institute of Standards and Technology (NIST) Special Publication 800-131A, and Supplier shall provide an automated remote key-establishment (update) method that protects the confidentiality and integrity of the cryptographic keys.

Part C: Cybersecurity Vulnerabilities, Assessment and Reporting

1. Supplier must develop and maintain an up-to-date Cybersecurity Vulnerability management plan designed to promptly identify, prevent, investigate, and mitigate any Cybersecurity Vulnerabilities and perform any required recovery actions to remedy the impact.

2. Supplier shall notify GE within a reasonable period, in no event to exceed five (5) business days after discovery, or shorter if required by applicable law or regulation, of any potential Cybersecurity Vulnerability. Supplier shall report any Cybersecurity Vulnerability to GE at ge.com/security, or at such contact information communicated to Supplier from time to time. Within a reasonable time thereafter, Supplier shall provide GE, free of charge, with any upgrades, updates, releases, maintenance releases and error or bug fixes necessary to remediate any Cybersecurity Vulnerability. Supplier shall reasonably cooperate with GE in its investigation of a Cybersecurity Vulnerability, whether discovered by Supplier, GE, or a third party, which shall include providing GE a detailed description of the Cybersecurity Vulnerability, the remediation plan, and any other information GE reasonably may request concerning the Cybersecurity Vulnerability, as soon as such information can be collected or otherwise becomes available. GE or GE's agent shall have the right to conduct a cybersecurity assessment of the applicable Products, and the Product development lifecycle, which includes tests intended to identify potential cybersecurity vulnerabilities. Supplier shall designate an individual responsible for management of the Cybersecurity Vulnerability, and shall identify such individual to GE promptly.

3. GE reserves the right to conduct an audit, upon 30 days advance notice, of Supplier's compliance with the requirements set forth herein, including but not limited to: (i) review of Supplier's applicable policies, processes, and procedures, and (ii) review of Supplier's sourcing processes.

4. Supplier shall have an incident management process to ultimately support the end user, including notification of the start and resolution of an incident. Incidents include, but are not limited to: physical security breach, and cyber security breach – e.g. network attack, virus infection etc.

5. Other than when required by law or regulation, Supplier may not make or permit any public statements concerning GE's involvement with any such Cybersecurity Vulnerability to any third-party without the explicit written authorization of GE's Legal Department.

Part D: Subcontracts

Subcontracts relating to Products must be approved by GE. Supplier must obligate approved subcontractors to comply with the applicable requirements herein and take reasonable steps to ensure continuing compliance by such subcontractors.

Part E: Training

Supplier shall provide training and ensure a process is in place to ensure its personnel and subcontractors have been informed of, accept and comply with GE's cyber security policies. Supplier personnel and subcontractors must undergo an awareness and role-based training program that promotes cyber security. This includes relevant security policies, procedures and awareness of industry standards (e.g. IEC62443). The training shall be given to personnel and subcontractors on a yearly basis at a minimum.

Part F: Physical Security and Distribution Integrity

The Supplier shall have a process to ensure appropriate physical and digital security mechanisms are in place, including, but not limited to, (i) allowing access to GE's components' environment only to personnel cleared by both supplier and GE; (ii) the use of tamper evident seals on media and containers, to detect unauthorized access to protected products (e.g. tamper evident labels or seals, which self-destruct and leave a residue sticker if removed); and (iii) tamper-resistant production (e.g. digital signatures for software and corresponding hardware mechanisms).

Part G: Additional Representations and Warranties

1. *Open Source Software and Third Party Materials Warranty*. Supplier represents, warrants and covenants that (i) it has disclosed all Open Source Software and Third Party Materials utilized with the Products, and no Open Source Software or Third Party Materials have been or will be provided to GE or used as a component of or in relation to any Products provided under the Agreement, except with the prior written authorization of GE; and (ii) all Open Source Software contained within the Products are and shall be in material compliance with the terms and conditions of the applicable licenses governing their use, and the Products or the use thereof by GE shall not cause GE or GE's intellectual property rights to be subject to the terms or conditions of a Copyleft License, or require GE to fulfil any open source license obligations for any Open Source Software contained within the Products.

2. *Code Integrity Warranty*. Supplier represents, warrants, and covenants that the Products: (a) do not contain any restrictive devices such as any key, node lock, time-out, time bomb, or other function, whether implemented by electronic, mechanical, or other means, which may restrict or otherwise impair the operation or use of the Products or any material embodying or comprising Products; and (b) shall be free of viruses, malware, and other harmful code (including, without limitation, time-out

features) which may interfere with the use of the Products regardless of whether Supplier or its personnel purposefully placed such code in the Products. In addition to exercising any of GE's other rights and remedies under this Agreement or otherwise at law or in equity, Supplier shall provide GE, free of charge, with any and all new versions, upgrades, updates, releases, maintenance releases, and error or bug fixes of the Products (collectively, "Revised Code") which prevents a breach of any of the warranties provided under this Agreement or corrects a breach of such warranties. Revised Code contained in the Products constitutes Products for purposes of this Agreement.

Part H: Additional Insurance

Supplier shall obtain Technology Errors & Omissions Liability Insurance, with a minimum limit of USD $5,000,000 per claim and in the aggregate, covering all Products including failure of IT security and data privacy breach and software copyright infringement. If coverage is on a claims-made basis, the policy must contain a retro date which precedes the effective date of this Agreement and continuity must be maintained for 1 year following termination or expiration of this Agreement.