

# ICT SCRM (NIST SP-800 161) Questionnaire

## 1. Contact Information

---

1.1 Third-Party Provider Name\*

1.2 Location of Data Center\*

1.3 Address\*

1.4 Location of Recovery Center

1.5 IT Security Contact

1.6 Phone\*

1.7 E-mail\*

1.8 Web site\*

1.9 Description of Service/Product (include technical details, e.g. client, agent, SSL, FTP transmission, hosted website, ASP, etc.)\*

1.10 Describe Pertinent Outsourced/Contracted Service Arrangements (e.g. onsite support, remote support, temporary access, database management, etc.)\*

## 2. Qualifying Questions

---

**2.1 Have you previously provided supply chain risk management information to this organization? If 'Yes' please provide an updated revision covering material changes.\***

**2.2 Do you have controls fully aligned to NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organization?\***

**2.2.1 Please provide proof of the scope of controls implemented and how controls were validated.\***

**2.2.2 Provide any additional supporting documentation of relevant and current third- party assessments or certification for supply chain risk management, such as ANSI/ASIS SCRM 1.2014, ISO 28000:2007, ISO 31000, ISO 20243, etc.\***

### 3. Supply Chain Management and Supplier Governance

---

#### General

**3.1 Do you have policies to ensure timely notification of updated risk management information previously provided to us? [Yes, No, Alternate, or N/A]\***

**3.1.1 How do you notify us of changes?\***

**3.1.2 What is your customer notification policy? \***

#### Information Communications Technology (ICT) Supply Chain Management

**3.2 Do you have a documented Quality Management System (QMS) for your ICT supply chain operation based on an industry standard or framework?\***

**3.2.1 Please provide the document which describes your QMS, including any standards or frameworks to which it is aligned.\***

**3.3 Do you have an organization-wide strategy for managing end-to-end supply chain risks (from development, acquisition, life cycle support, and disposal of systems, system components, and to system services)?\***

**3.3.1 What is your strategy?\***

**3.3.2 How have you implemented it?\***

#### Authentication and Provenance

**3.4 Do you have a policy or process to ensure that none of your suppliers or third-party components are on any banned list?\***

**3.5 Do you provide a bill of materials (BOM) for your products, services, and components which includes all logic-bearing (e.g., readable/writable/programmable) hardware, firmware, and software?\***

- 3.5.1 If you provide a BOM that does not include all logic-bearing hardware, firmware, and software, what does your BOM include?\***
- 3.5.2 Upon request, are you able to provide your BOM including all logic-bearing hardware, firmware, and software?\***
- 3.5.3 How do you track changes in your products, services, and components and how do you reflect those changes in the applicable BOM(s)? How do you track changes in your products, services, and components and how do you reflect those changes in the applicable BOM(s)?\***
- 3.6 For hardware components included in the product offering, do you only buy from original equipment manufacturers or licensed resellers?\***
- 3.7 Do you have a process for tracking and tracing your product while in development and manufacturing?\***
- 3.7.1 How do you keep track of your chain of custody?\***
- 3.7.2 How do you track and trace components within your product?\***

## **Supplier Governance**

- 3.8 Do you have written Supply Chain Risk Management (SCRM) requirements in your contracts with your suppliers?\***
- 3.8.1 What are your SCRM requirements?\***
- 3.8.2 How do you verify that your suppliers are meeting contractual terms and conditions, which may include requirements to be passed down to sub-suppliers?\***
- 3.8.3 If violations of contractual SCRM requirements or SCRM-related incidents occur, do you ensure and monitor any remediation activities?\***

**3.9 Do you revise your written SCRM requirements regularly to include needed provisions?\***

**3.10 Do you have policies for your suppliers to notify you when there are changes to their subcontractors or their offerings (components, products, services, or support activities)?\***

**3.10.1 Please describe your policy.\***

## 4. Secure Design And Engineering

---

### General

4.1 Does your organization develop (or integrate) custom hardware or software offerings?\*

4.1.1 List the custom software, hardware, system, or solution offering(s) provided by your organization \*

### Protect IP and Product (Supplier) Offering Assets

4.2 Does your organization protect all forms of code from unauthorized access and tampering, including patch updates? \*

4.2.1 How does your organization prevent unauthorized changes to code, both inadvertent and intentional, which could circumvent or negate the intended security characteristics of the software?

\*

4.3 Does your organization provide a mechanism for verifying software release integrity, including patch updates for your software product offering? \*

4.4 How does your organization prevent malicious and/or counterfeit IP components within your product offering or solution? \*

4.5 Does your organization manage the integrity of IP for its product offering.\*

4.5.1 How does your organization archive assets associated with the product offering development or manufacturing process? \*

### Secure Coding and Manufacturing Practices

4.6 Does your organization define, follow, and validate secure coding and manufacturing practices to mitigate security risks?\*

- 4.6.1 How does your organization conduct threat modeling to determine required product offering security requirements? \***
- 4.6.2 How does your organization determine how identified risks are mitigated in product offering design?\***
- 4.6.3 How does your organization justify risk-based decisions to relax or waive security requirements or controls? \***
- 4.6.4 How does your organization validate that the offering will meet the security requirements and satisfactorily address the identified threat assessment? \***
- 4.7 Does your organization verify that third-party software provides required security requirements/controls?\***
- 4.7.1 How does your organization reduce the risk associated with using acquired software modules and services, which are potential sources of additional vulnerabilities?\***
- 4.8 Does your organization reuse existing, well-secured software and hardware components, when feasible, instead of duplicating functionality?\***
- 4.9 Does your organization configure the compilation and build processes to improve executable security?\***
- 4.9.1 How does your organization decrease the number of security vulnerabilities in the software and reduce costs by eliminating vulnerabilities before testing occurs?\***
- 4.10 Does your organization implement formal vulnerability and weakness analysis practices?\***
- 4.10.1 Does your organization automate the identification of security vulnerabilities and weaknesses?\***
- 4.10.2 Does your organization test executable code or components to identify vulnerabilities and verify compliance with security requirements?\***

**4.11 Does your organization configure offerings to implement secure settings by default?\***

**4.11.1 Does your organization test offerings using hardened runtime environments?\***

**4.12 Does your organization maintain and manage a Product Security Incident Reporting and Response program (PSIRT)?\***

**4.12.1 How does your organization assess, prioritize, and remediate reported vulnerabilities?\***

**4.12.2 How does your organization ensure that vulnerabilities are remediated in a timely period, reducing the window of opportunity for attackers?\***

**4.13 Does your organization analyze vulnerabilities to identify root cause?\***

**4.13.1 Are vulnerability root causes used as input to update secure development process, tools, and training to lower future vulnerabilities?\***

## 5. Information Security

---

### General

5.1 Do you hold a valid information security/cybersecurity third-party attestation or certification? (e.g., ISO 27001, SOC 2 Type 2, CMMC Level 3-5, Cybersecurity Maturity Assessment, etc.)\*

5.2 Do you follow operational standards or frameworks for managing Information Security/Cyber security? (e.g., NIST CSF 1.1, NIST 800-37, Rev. 2, NIST SP 800-161, ISO IEC 27001, ISO 20243, ISO 27036, SAE AS649)\*

5.2.1 If so, please state which one(s)?\*

5.3 Do you have company-wide, publicly available information security policies in place covering privacy policies?\*

5.3.1 If 'Yes', please provide.\*

5.3.2 What mechanisms are in place to ensure your policies are enforced within your supply chain?\*

5.3.3 Do you receive notification of and have a response plan in place for privacy violations of the suppliers in your supply chain?\*

### Asset Management

5.4 Do you inventory and audit back-up and/or replacement hardware and software assets to ensure their accountability and integrity?\*

5.4.1 What recognized standards or frameworks do you follow to ensure integrity of back- up assets? (e.g., NIST 800-53, NIST 800- 171 DFARS, ISA/IEC 62443 or ISO 27001/2)\*

5.5 Do you have a defined governance scope for asset management, including line of business technology, facilities, devices, and all other data- generating hardware (like Internet of Things devices)?\*

**5.6 Do you have processes or procedures in place to ensure that devices and software installed by users external to your IT department (e.g., line of business personnel) are being discovered, properly secured, and managed?\***

**5.6.1 What, if any, types of assets are out of scope for your tracking procedures?\***

**5.7 Do you have an asset management program approved by management for your IT assets that is regularly maintained?\***

**5.7.1 What are your methods to manage IT assets on the network?\***

**5.7.2 How do you manage other IT hardware and software assets which are not network connected, regardless of network presence?\***

**5.7.3 What are your methods of verifying acceptable use of assets, including verified asset return, for your network-connected assets?\***

**5.8 Do you have documented policies or procedures to manage enterprise network-connectable assets throughout their lifecycle?\***

**5.8.1 What are your processes to manage obsolescence of network-connected assets?\***

**5.8.2 What are your policies or procedures to ensure your enterprise software platforms and applications, and hardware assets, are classified according to their criticality?\***

**5.8.3 What are your policies or procedures to ensure appropriate controls are in place for internal or third-party cloud services?\***

**5.9 Do you ensure that you are not sourcing assets on a banned list to customers (e.g., ITAR, NDAA Section 889)?\***

**5.9.1 How do you ensure that you are not providing assets on a banned list to customers?\***

**5.10 Do you have documented hardware and software policies and practices in place to ensure asset integrity?\***

**5.10.1 What recognized standards or frameworks are followed to ensure asset integrity?\***

**5.10.2 How do you ensure that regular reviews and updates of the asset integrity policies and practices are performed?\***

## **Identify**

**5.11 Do you have documented policies or procedures for identification and detection of cyber threats?\***

**5.11.1 What processes do you have in place to promptly detect cyber threats?\***

**5.11.2 How do you manage the identification of threats within your supply chain, including suppliers and sub-contractors?\***

**5.11.3 What processes are in place to act upon external credible cyber security threat information received?\***

**5.12 Do you address the interaction of cybersecurity operational elements (e.g., SOC, CSIRT, etc.) with the physical security operational elements protecting the organization's physical assets?\***

**5.12.1 How do you ensure that physical security incidents and suspicious events are escalated to cybersecurity operations staff?\***

**5.12.2 Are cybersecurity vulnerabilities for industrial control systems, including physical access controls and video monitoring systems, tracked?\***

**5.12.3 What standards or frameworks are followed for management of IT and OT system interactions?\***

**5.13 Do you have a policy or procedure for the handling of information that is consistent with its classification?\***

**5.13.1 What is your process to verify that information is classified according to legal, regulatory, or internal sensitivity requirements?\***

**5.13.2 How do you convey requirements for data retention, destruction, and encryption to your suppliers?\***

**5.14 Do you have documented policies or procedures for internal identification and management of vulnerabilities within your networks and enterprise systems?\***

**5.14.1 What industry standards or frameworks are followed for vulnerability management?\***

**5.14.2 How do you identify vulnerabilities in your supply chain (suppliers/sub- contractors) before they pose a risk to your organization?\***

**5.14.3 How do you assess and prioritize the mitigation of vulnerabilities discovered on your internal networks and systems? (e.g., asset criticality, exploitability, severity, etc.)\***

## **Protect**

**5.15 Do you have network access control policies and procedures in place for your information systems that are aligned with industry standards or control frameworks?\***

**5.15.1 If Yes, please list any standards or frameworks used.\***

**5.15.2 What are your practices for items such as federation, privileged users, and role- based access control for end-user devices?\***

**5.15.3 How do you ensure remote access is managed for end-user devices or employees and suppliers, including deactivation of accounts? (e.g. Multi-factor authorization, encryption, protection from malware, etc.)\***

**5.15.4 How do you identify and correct end-user systems that fall out of compliance?\***

**5.16 Is cybersecurity training required for personnel who have administrative rights to your enterprise computing resources?\***

**5.16.1 What is the frequency for verifying personnel training compliance?\***

**5.16.2 What cybersecurity training is required for your third-party stakeholders (e.g., suppliers, customers, partners, etc.) who have network access?\***

**5.16.3 How is training compliance tracked for third parties with network access?\***

**5.17 Do you include contractual obligations to protect information and information systems handled by your suppliers?\***

**5.17.1 What standard cybersecurity standards or frameworks are the contractual supplier terms for information protection aligned to, if any?\***

**5.18 Do you have an organizational policy on the use of encryption that conforms with industry standards or control frameworks?\***

**5.18.1 What industry standards or controls frameworks are followed for encryption and key management?\***

**5.18.2 What processes or procedures exist to comprehensively manage the use of encryption keys?\***

**5.18.3 What is your process for protecting data at rest and in transit?\***

**5.19 Does your organization have hardening standards in place for network devices (e.g., wireless access points, firewalls, etc.)?\***

**5.19.1 What protections exist to provide network segregation where appropriate (e.g., intrusion detection systems)?\***

**5.19.2 What controls exist to continuously monitor changes to your network architecture (e.g., NIST 800-53 or related controls)?\***

**5.19.3 How do you manage prioritization and mitigation of threats discovered on your networks?\***

**5.19.4 How do you track changes to software versions on your servers?\***

**5.20 Do you follow an industry standard or framework for your internal or third- party cloud deployments, if applicable?\***

**5.20.1 What protections are in place between your network and cloud service providers?\***

**5.20.2 How to do you convey cloud security requirements to your suppliers/sub-contractors?\***

## **Detect**

**5.21 Do you have defined and documented incident detection practices that outline which actions should be taken in the case of an information security or cybersecurity event?\***

**5.21.1 Are cybersecurity events centrally logged, tracked, and continuously monitored?\***

**5.21.2 Are incident detection practices continuously improved?\***

**5.22 Do you require vulnerability scanning of software running within your enterprise prior to acceptance?\***

**5.22.1 What procedures or policies exist, if any, for detecting vulnerabilities in externally obtained software (such as penetration testing of enterprise and non-enterprise software)?\***

**5.22.2 What are your procedures to scan for vulnerabilities in supplier-provided software running on your network?\***

**5.23 Do you manage updates, version tracking of new releases, and patches (including patching history) for your software and software services offerings?\***

**5.23.1 What is the responsibility of the product end-user (customer) for updating software versions?\***

**5.24 Do you deploy anti-malware software? [Yes, No, Alternate, or N/A]\***

**5.24.1 What systems are out of scope for anti-malware software compliance, if any?\***

**5.24.2 How do you ensure anti-malware is present on developer platforms? As applicable to your offering?\***

## **Respond & Recover**

**5.25 Do you have a documented incident response process and a dedicated incident response team (CSIRT - Computer Security Incident Response Team)?\***

**5.25.1 What is your process for reviewing and exercising your resiliency plan?\***

**5.25.2 What is your process to ensure customers and external entities (such as government agencies) are notified of an incident when their product or service is impacted?\***

**5.26 Do you have processes or procedures to recover full functionality, including integrity verification, following a major cybersecurity incident?\***

**5.26.1 What is the frequency for testing of back-up media?\***

**5.27 Do you insure for financial harm from a major cybersecurity incident (e.g., self-insure, third- party, parent company, etc.)?\***

**5.27.1 Does coverage include financial harm to your customers resulting from a cybersecurity breach which has impacted your company?\***

## 6. Physical Security

---

### General

- 6.1 Is the entity (organization, operational unit, facility, etc.) currently covered by an unrestricted/unlimited National Industrial Security Program (NISP) Facility Clearance (FCL) or a related U.S. government program such as C-TPAT that certifies the entity as meeting appropriate physical security standards?\*
- 6.1.1 If the entity is not covered by a NISP FCL but currently has some other US Government or industry attestation, such as TAPA FSR of meeting a physical security code or standard, please identify the standard, the issuing agency, and the most recent date of certification.\*
- 6.1.2 Is the entity covered by a limited FCL (in agreement with a foreign government)? Describe.\*
- 6.2 Do you have documented security policies and procedures that address the control of physical access to cyber assets (network devices, data facilities, patch panels, industrial control systems, programmable logic, etc.)?\*
- 6.2.1 To what standards/controls do you adhere? (e.g., NIST publication, ISO, UL, etc.)\*
- 6.2.2 How often do you review and update to those policies and procedures and what is the most recent review?\*
- 6.2.3 If needed, can you provide these documents for our review?\*
- 6.3 Do you have documented policies addressing staff training which includes procedures to limit physical access to cyber assets to only those with demonstrated need?\*
- 6.3.1 What training do all staff receive to address potential physical security threats and how to respond to emergencies (e.g., fire, weather, etc.)?\*
- 6.3.2 What training do cybersecurity staff, physical security staff, and contractors with at least limited access to sensitive areas of a facility receive?\*
- 6.3.3 How does this training address potential threats to the facility and how the physical access controls are integrated with system network interfaces?\*

**6.3.4 What standards do you follow, or did you implement (e.g., NIST publication, ISO, UL, etc.)?\***

**6.3.5 How is this training documented?\***

**6.4 Do you have a documented Security Incident Response process covering physical security incidents? (e.g., potential intruder access, missing equipment, etc.)?\***

**6.4.1 What processes do you have in place to document the actions taken during and after an actual or suspected physical security incidents (e.g., security log, formal report to management, police report, etc.)?\***

**6.4.2 How do you ensure that your staff understands and complies with procedures (e.g., training, exercises, and actual cases of incident response)?\***

**6.5 For facilities that use an independent contractor for physical security, are physical facilities security policy and procedures incorporated into service level agreements, contracts, policies, regulatory practices?\***

**6.5.1 What physical / facilities security policies and practices are subject to audit?\***

**6.5.2 What physical / facilities security policies and practices are subject to audit?\***

**6.5.3 How is compliance with these standards validated?\***

**6.6 Are there enforcement mechanisms (e.g., sanctions, response procedures, technology) for unauthorized physical access to mission/business critical information, functions, services and assets?\***

**6.6.1 What type of action or response would be taken for unauthorized physical access to sensitive cyber assets?\***

**6.7 Do you have evidence that physical security mechanisms are effective and adequate to protect assets? Evidence could include third-party assessment, self-assessment, records of actions taken to enforce rules, etc.\***

**6.7.1 What is the date of the last review and update to your enforcement strategy?\***

## **Physical Security In-transit**

**6.8 Do you utilize a controlled bill of materials (BOM) or similar capability to protect assets that are being received, in process, or in-transit?\***

**6.8.1 What industry standards or frameworks are followed?\***

**6.9 Do you have requirements that all items being shipped have tamper-evident packaging?\***

**6.9.1 What industry standards or frameworks are being followed to ensure packaging is tamper-evident?\***

**6.9.2 What industry standards or frameworks are being followed to ensure packaging is tamper-evident?\***

**6.10 Do you have processes in place to prevent counterfeit parts from entering your supply chain?\***

**6.10.1 What requirements, if any, are in place to ensure the use of Original Equipment Manufacturer (OEM) or Authorized Distributors for all key components?\***

**6.10.2 What requirements, if any, are in place to ensure the use of Original Equipment Manufacturer (OEM) or Authorized Distributors for all key components?\***

**6.10.3 How do you pass on counterfeit prevention requirements to your third- party suppliers?\***

## 7. Personnel Security

---

### General

7.1 Does a formal personnel security program exist? \*

7.1.1 Is employee access managed by role?\*

7.1.2 Are physical security practices formally governed, documented, maintained, and enforced?\*

### Onboarding

7.2 Do you have a process for onboarding personnel?\*

7.2.1 Does the process include security awareness training?\*

7.2.2 What is the process to determine the level of access to company identifications (IDs), tokens, documents, applications, etc.?\*

7.2.3 What is the process to distribute company assets?\*

7.2.4 Is the onboarding process documented?\*

7.2.5 If 'Yes', please provide a copy.\*

7.3 Do you have policies for conducting background checks of your employees as permitted by the country in which you operate?\*

7.3.1 If not permitted by the country, please note that and provide the part of your supply chain for which it is applicable.\*

7.3.2 How do you conduct the background checks and document, validate, and update their responses?\*

**7.4 Do you have policies for conducting background checks for your suppliers, as permitted by the country in which you operate?\***

**7.4.1 If not permitted by the country, please note that and provide the part of your supply chain for which it is applicable.\***

**7.4.2 How do you conduct the background checks and document, validate, and update their responses?\***

**7.5 Do you have policies for conducting background checks for any subcontractors, as permitted by the country in which you operate?\***

**7.5.1 If not permitted by the country, please note that and provide the part of your supply chain for which it is applicable.\***

**7.5.2 How do you conduct the background checks and document, validate, and update their responses?\***

\*

## **Offboarding**

**7.6 Do you have a process for offboarding personnel?\***

**7.6.1 Does the process include a process to transfer knowledge to other personnel?\***

**7.6.2 Does the process include a process to transfer knowledge to other personnel?\***

**7.6.3 What is the process to recover all company assets?\***

**7.6.4 Is that process documented?\***

## **Awareness and Training (Security-Specific)**

**7.7 Are personnel security practices formally documented and accessible to all employees?\***

**7.8 Are Personnel Security practices routinely enforced, audited, and updated?\***

**7.9 Are personnel required to complete formal SCRM training annually?\***

**7.10 Are all personnel trained in security best practices? This includes, but is not limited to, insider threats, access control, and data protection.\***

**7.11 Is there additional security training provided to users with elevated privileges?\***

**7.12 Are you aware of security training practices performed by your sub-suppliers to their personnel?\***

**7.12.1 If 'Yes', does it align with your security practices?\***

**7.13 Do you have a Code of Conduct for your employees, suppliers and subcontractors?\***

**7.13.1 Is the Code of Conduct always available and visible to your employees, suppliers, and subcontractors?\***

**7.13.2 How [regularly or often] is this Code of Conduct updated? Please describe the frequency.\***

**7.13.3 Do you have personnel designated to address questions or violations to the Code of Conduct?\***

**7.13.4 Are these employees, suppliers, and subcontractors trained on the Code of Conduct, including privacy and confidentiality requirements, as required by your industry?\***

## 8. Supply Chain Integrity

---

**8.1 Do your processes for product integrity conform to any of the following standards (e.g., ISO 27036, SAE AS6171, etc.)?\***

**8.2 Do you control the integrity of your hardware/software (HW/SW) development practices by using Secure Development Lifecycle practices?\***

**8.2.1 How do you manage the conformance of your third parties to your procedures?\***

**8.3 Do you have documented performance and validation procedures for your HW/SW products or services?\***

**8.3.1 What is your process to ensure conformance to those procedures?\***

**8.3.2 How do you manage HW/SW products or service that are not in compliance with those procedures?**

\*

**8.3.3 How are subcontractors held accountable to performance specifications?\***

**8.3.4 What, if any, automated controls are in place for your validation processes?\***

**8.3.5 How do you audit your validation processes?\***

**8.4 Do you have processes in place to independently detect anomalous behavior and defects in HW/SW products or services?\***

**8.4.1 What means do you provide to allow customers to report anomalies?\***

**8.4.2 How do you monitor and track anomalous product or service behavior?\***

**8.5 Do you monitor third-party HW/SW products or services for defects? \***

**8.5.1 What are your processes for managing third-party products and component defects throughout their lifecycle?\***

**8.6 Does the functional integrity of your product or services rely on cloud services (commercial or hybrid)?\***

**8.6.1 What policies and procedures are in place to protect the integrity of the data provided through cloud services?\***

**8.6.2 How do you manage the shared responsibility for cloud service integrity requirements with your suppliers?\***

**8.7 Do you have required training on quality and product integrity processes for employees, suppliers, and subcontractors?\***

**8.7.1 What mechanisms are in place for direct employees and contracted workers to ensure applicable training has been completed?\***

**8.7.2 Do you pass down training requirements to your sub-suppliers, as applicable?\***

**8.8 Do you have processes to evaluate prospective third-party suppliers' product integrity during initial selection?\***

**8.8.1 What processes or procedures, if any, are in place to ensure that prospective suppliers have met your product integrity requirements?\***

**8.8.2 How do your policies or procedures ensure appropriate management/leadership input on supplier selection decisions?\***

**8.9 Do you have regularly scheduled audits to ensure compliance with HW/SW products or services integrity requirements?\***

**8.9.1 What provisions for auditing are included within supplier contracts?\***

**8.9.2 How do you pass down HW/SW products or services integrity requirements to third- party suppliers?\***

**8.10 Do you have a process for improving integrity of HW/SW products or services? \***

**8.10.1 What programs are in place to ensure continuous performance monitoring and improvement of key suppliers?\***

**8.11 Do you have processes in place for addressing reuse and/or recycle of HW products?\***

**8.11.1 What is your process?\***

## 9. Supply Chain Resilience

---

### General

**9.1 Does your organization have a formal process for ensuring supply chain resilience as part of your product offering SCRM practices?\***

**9.1.1 What standards or industry frameworks do you use to help inform those practices?\***

**9.2 Do you consider non-technical supply chain resilience threats such as weather, geo-political instability, epidemic outbreak, volcanic, earthquakes, etc.?\***

### Supply Chain Disruption Risk Management (Business Continuity)

**9.3 Do you maintain a formal business continuity plan necessary to maintain operations through disruptions and significant loss of staff?\***

**9.3.1 If illness causes high absenteeism, are personnel cross-trained and able to perform multiple duties?\***

**9.4 Do you maintain a formally trained and dedicated crisis management team, including on-call staff, assigned to address catastrophic or systemic risks to your supply chain or manufacturing processes?\***

**9.4.1 Do you require and audit key suppliers for their ability to be prepared for unexpected supply chain disruptions?\***

**9.5 Can personnel work remotely?\***

**9.5.1 Do your service deliverables outline which services can be done remotely and which cannot?\***

**9.5.2 Is that documented in Service-level agreement (SLA) or Terms and Conditions?\***

**9.5.3 What infrastructure support is needed to support a shift to an at-home workforce?\***

## Diversity of Supply Base

**9.6 Does your company consider supplier diversity to avoid single sources and to reduce the occurrence of suppliers being susceptible to the same threats to resilience?\***

**9.7 Does your company consider alternate offering delivery channels to mitigate extended supplier outages to include cloud, network, telecommunication, transportation, and packaging?\***