Appendix 2 - Vendor Specific Requirements for Supply Chain Security

This annex is providing the expectations and associated taxonomy for supply chain security for a vendor of CIS Security Enforcing Products to NATO.

1. This section describes the practices applicable to the portions of such vendors' Value Chains as identified in the Scope Section.

2. These practices provide a framework regarding supply chain security areas and steps to be deployed, as applicable, by all suppliers and vendors of CIS products to NATO. Through the procurement process the final vendor will establish a supply chain security self-attestation statement. Annex A of this directive provides a template.

3. These practices address the following key security areas applicable to the supply chains of vendors of CIS to NATO:

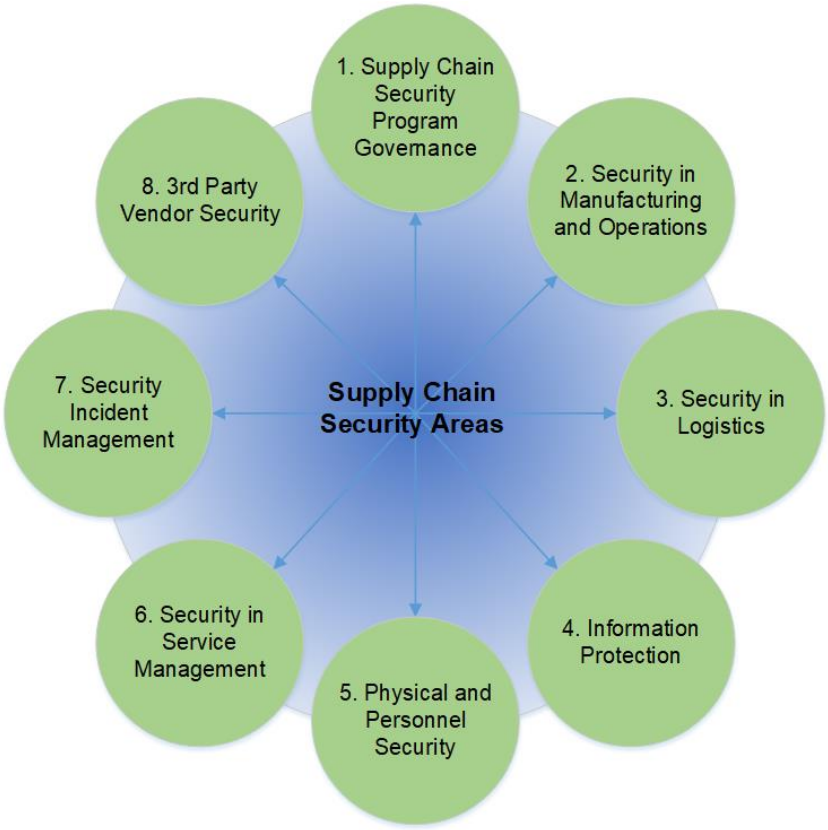

Figure 1 – Supply Chain Security Areas

1.1. Supply Chain Security Program Governance

1.1.1. This area of security describes the practices for a CIS product vendor's overall governance for supply chain security and compliance. The program shall cover the following issues:

- Governance model:
  - Clearly defining roles and responsibilities
  - Taking into account key third party vendor and their supply chain security conformance
- Security policies, standards and procedures:
  - Include supply chain security issues in their quality baseline, especially dealing with delivery and manufacturing issues;
  - Maintain a supplier management procedure in their quality baseline;
  - Security incident response procedures;
  - Define supply chain security self-assessment and internal audit processes.

1.1.2. The vendor, to improve its practices, should:

- Develop and implement a supply chain security program including roles and responsibilities, with identifying clearly 3rd party vendor.
- Conform with existing standard and practices like Assurance Life Cycle (ALC) assurance requirements of ISO/IEC 15408, Informational Technology – Security techniques – Evaluation criteria for IT security.
- Develop its policies to manage supply chain security risks in the following areas:
  - Manufacturing and service operations
  - Implementation control and validation processes
  - Scrap management processes
  - Cyber threat and vulnerability management
  - Anomaly detection and investigation
  - Counterfeit mitigation, integrity and trapping
  - Compliance management to manufacturing specification note
  - Conduct short-periodic assessments by independent third parties against supply chain security leading practices to identify potential gaps

1.2. Security in Manufacturing and Operations

The governed supply chain security program shall address security in manufacturing and operations.

1.2.1. The area of security in manufacturing and operations describes the practices to protect against supply chain security threats and risks in manufacturing operations. It shall address, at least, the following:

- Security of production platform
- Security in Inventory Management
- Segregation of Duties
- Tracking and Accountability
- Scrap Management
- Tampering and Malicious Modification
- Counterfeit Mitigation

1.2.2. The CIS product vendor, to improve its practices, should:

- Implement controls to manage access to material inventory within the

production environment.
- Maintain accounting of inventory throughout the production lifecycle.
- Maintain inventory tracking documentation and/or information for an appropriate agreed time period.
- CIS equipment/components should be marked with one or more markers such as company logo, forgery-proof part number to prevent counterfeiting.
- Implement applicable separation of duties controls to limit opportunities for counterfeiting, malicious modification and tampering.
- Scrap should be tracked and controlled until destroyed or deemed unusable.

1.3. Security in Logistics

The governed supply chain security program shall address security in logistics.

1.3.1. The area of security in logistics describes the practices to protect against security threats and risks during storage and distribution of software, components and products through the supply chain. It shall address, at least, the following:

- Packaging Security
- Transportation Security, including tampering detection
- Secured Warehousing and Storage

1.3.2. The CIS product vendor, to improve its practices, should:

- Ensure anonymity of client by implementing technical mechanism that does not require to show human-readable or direct information about client (example given: bar-code…).
- Implement a control policy for each equipment/component before their packaging.
- Ensure robust tamper detection by advanced mechanism (seal, secure packaging…)
- Implement anti-tamper mechanisms
- Store proprietary material in an access controlled area.
- Uniquely identify all shipped components using valid identification and tracking techniques (e.g., serial numbers, date codes, license labels).

1.4. NATO Procurement and Sustainment Information Protection

The governed supply chain security program shall address NATO procurement and sustainment information protection.

This area addresses the protection of all NATO information handled during the operation of the CIS product and all the services linked to its usage. It covers information related to the support service and the hotline involved in the maintenance of the product during the sustain phase; information required by an ancillary service, like signature pushing, necessary for the correct operation of the product and any residual information in equipment handled all along the sustain and end-of-life phases and scrap management.

The vendor shall address these issues by:

- Using of cryptographic mechanisms and products to protect sensitive information exchanged
- Setting up information access controls
- Enforcing a network security policies regarding confidentiality consistent with the sensitivity data handled, which may include parameters for use of third party cloud service providers.

1.4.1. The CIS product vendor, to improve its practices, should:

- Secure and control NATO and procurement and sustainment information in a manner such that:
  - It limits the use for intended purpose;
  - Limits the access to authorized personnel compliancy with need-to-know concept and cleared at the appropriate NATO level;
  - Ensures segregation from that of other customers (e.g. separate information system customer directories).
- Ensure confidentiality of information during storage, scrapping and while in transit, using techniques as permitted by NATO directives.
- Implement all procedures and technical measures to prevent leakage of NATO procurement and sustainment information.
- Ensure anonymization or confidentiality of shipping and information gathered during the support and maintenance phases.
- Periodically have access control procedures, including visitor access, and all technics used to prevent leakage of information audited by independent control office.
- Ensure confidentiality of design and development information that could jeopardize product security.

1.5. Vendor Physical and Personnel Security

The governed supply chain security program shall address vendor physical and personnel security.

1.5.1. This area of personnel security describes the practices to protect NATO's operational or business confidential information when employees and contractors have physical access to such information on vendor premises. It shall address, at least, the following:

- Physical Access Controls and Monitoring, in compliance with NATO directive protection of such a confidential information at proper level.
- Security training and awareness, in compliance with NATO directive on protection of such a confidential information at proper level.

1.5.2. The CIS product vendor, to improve its practices, should:

- Implement applicable physical access controls for entering as well as exiting facilities.
- Periodically have development and loading premises, including all remote network access point audited by independent control office.
- Periodically review and update physical access entitlement and privilege. This review should be based on employee background, adjusting the roles.

- Deploy periodic security awareness campaigns and training to all personnel addressing the following areas, as applicable:
  - Security and information protection practices against social engineering, phishing, malware, etc.
  - Information systems access
  - Security incident detection and reporting
  - Response to burglary, robbery and in-transit theft
  - Visitor access and challenging unidentified persons or vehicles
  - Management and disposal of scrap
  - Detection of counterfeit items and malicious modification

1.6. Security in Service Management

The governed supply chain security program shall address security in service management.

1.6.1. This area of service management describes the practices to continue to securely deliver support and ancillary services required for the security product to be operated – e.g. online services like signature server – and maintained – e.g. online update server – in an event of a service disruption. It shall address, at least, the following:

- Security in Business Continuity Planning issues;
- Business Continuity Plan Testing procedures;
- Activity Recovery Plan.

1.6.2. The CIS product vendor, to improve its practices, should:

- Implement security controls as part of business continuity efforts (e.g. processes, location) to ensure confidential information is protected during periods of disruption.
- Implement vulnerability survey, both from customers and open sources.
- Post-sale services and configuration support.
- Test business continuity plans for security periodically and update them based on the results of the testing.

1.7. Security in Incident Management

The governed supply chain security program shall address security in incident management.

1.7.1. This area of security incident management describes the practices to establish and implement a robust incident management process to identify, document and resolve security incidents. It shall address, at least, the following:

- Incident handling and response procedures

1.7.2. The CIS product vendor should:

- Establish capabilities to identify and respond to security incidents.
- Assign roles and responsibilities to personnel, including response procedures, to manage security incidents effectively.
- Review incident response plan periodically and update based on evolving

security risks and threats.
- Vulnerability review and impact analysis on CIS product facilities.
- Implement analysis of 0-day incidents, including their impact on the supply chain.

1.8. 3rd Party Supplier Management

The governed supply chain security program shall address 3rd party supplier management.

1.8.1. This area of 3rd party security describes making multiple tiers of suppliers to a CIS product vendor to NATO aware of all applicable security practices. The prior vendor shall ask to their 1st tier of underlying suppliers/partners for an assessment of the suppliers' supply chain security expressing compliance to this directive. Direct vendors to NATO should make supply chain security statement of their underlying suppliers available to the contracting authorities.

1.8.2. Direct vendors to NATO should provide 3rd party suppliers with this directive and make them aware of its content, both requirements and recommended practices.

For information purposes only.