CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

OPERATIONALIZING THE VENDOR SUPPLY CHAIN RISK MANAGEMENT TEMPLATE FOR SMALL AND MEDIUM-SIZED BUSINESSES

September 2021

This page is intentionally left blank.

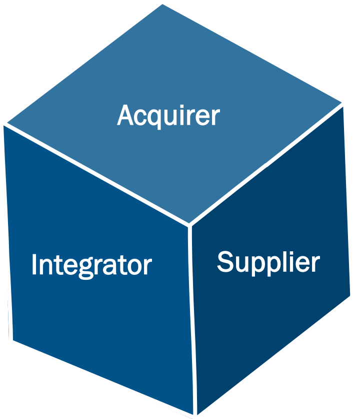
OPERATIONALIZING THE VENDOR SUPPLY CHAIN RISK MANAGEMENT TEMPLATE FOR SMALL AND MEDIUM-SIZED BUSINESSES

Executive Summary

The 31.7 million small and medium-sized businesses (SMBs) across the United States account for 41.7 percent of private sector employees and nearly half of the nation's gross domestic product.[i] The Information and Communications Technology Supply Chain Risk Management (ICT SCRM) Task Force (Task Force) established an SMB working group (Working Group) to focus on the specific ICT supply chain needs of IT and Communications SMBs. For the purposes of this report, IT or Communications small or medium-sized businesses are defined as, "Organizations with up to 500 employees while expecting most of these organizations to have fewer than 100 employees."[ii]

The Working Group identified use cases commonly encountered by small and medium-sized IT and communications providers, using the ICT SCRM Vendor Supply Chain Risk Management Template ("Vendor Template").[iii] This template includes standardized questions intended to communicate ICT supply chain risk posture from the perspective of the Acquirer, Integrator, and Supplier in order to achieve better outcomes as reflected in figure 1.

Figure1: Three Roles that Small and Medium-sized Businesses Assume



- Acquirer – An SMB owner/operator/executive that aims to make a purchase where ICT supply chain security is of concern.
- Integrator – An SMB integrator acquiring and implementing ICT products or services on behalf of their clients.
- Supplier – An SMB business owner/operator/executive that aims to win a contract where ICT supply chain security is of concern to the prospective client.

The Working Group viewed the Vendor Template from the perspective of an IT or Communications SMB, selecting one or more perspectives described above as applicable to each of the identified use cases, and documented the benefits and desired outcomes for the use case for each

[i] https://cdn.advocacy.sba.gov/wp-content/uploads/2020/11/05122043/Small-Business-FAQ-2020.pdf
[ii] *Definitions for Small- and Medium-Sized Business.* (2021). Washington, DC: IT Sector Coordinating Council
[iii] https://www.cisa.gov/publication/ict-scrm-task-force-vendor-template

selected perspective. The Working Group then selected, **verbatim** from the Vendor Template, those questions that were **most relevant and important** to the use cases **with respect to IT and Communications SMBs**. If an SMB is using multiple use cases, it may be helpful to identify common questions among them. Answers to the questions might rest somewhere between “yes” and “no.” As a result, Appendix B includes a list of resources SMBs can use to identify methods of increasing their supply chain security. Appendix C, incorporated by reference, is an accompanying spreadsheet that contains the same questions selected in each use case and presented in an alternate format.

OBJECTIVE:

This product assists in mitigating ICT supply chain risk with a specific focus on making the enterprise Vendor Template more accessible and usable for SMBs.

SCOPE:

The Working Group selected three commonly encountered use cases that will help identify supply chain risks, including threats and vulnerabilities as they relate to the National Vulnerability Database.[iv] The ICT SCRM Task Force Threat Evaluation Working Group published an extensive list of threat scenarios and potential mitigations for those threats.[v] While it is important for businesses to consider all threats to their supply chain, limited resources dictate assessing and prioritizing threats that pose the highest risk and potential consequences. Once an organization mitigates identified threats to the best of the organization's ability, it should consider additional threats on an ongoing basis.

METHODOLOGY:

The Working Group identified several use case scenarios and narrowed them down to the three use cases included in this report as a starting point. Each use case identified specific questions from the Vendor Template and outlined which questions pertained to the role of Acquirer, Integrator, or Supplier.

[iv] https://nvd.nist.gov/

[v] https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v2.pdf

Contents

Figures

SMALL TO MEDIUM-SIZED BUSINESSES (SMBs) WORKING GROUP

We thank the Working Group and the entire Task Force for their participation, and a special thank you to those listed below who participated in the Writing Teams:

Leadership Team:

	Name	Organization
Co-Chair	Ola Sage	CyberRx
Co-Chair	Robert Arnold	DHS CISA
Co-Chair	Tamber Ray	NTCA - The Rural Broadband Association

Writing Team participants:

Name	Organization
Andras Szakal	The Open Group
Chad Kliewer	Pioneer
Frank Bulk	Premier Communications
Jack Nemceff, Valerie Dumas	Dept. of State
Jeffery Goldthorp, Zenji Nakazawa	Federal Communications Commission
Jerry Horton	Blue Valley Inc.
John Minasyan	Belkin International
Kathryn Basinsky, Megan Doscher	National Telecommunications and Information Administration
Rebecca Adams, Jennifer Hunt, Briana Alston	DHS CISA

USE CASE 1

APPLYING ICT VENDOR SUPPLY CHAIN RISK MANAGEMENT TO PHYSICAL OR LOGICAL ACCESS CONTROLS

Description

Risk is introduced anytime a small or medium-sized business (SMB) grants physical or logical access to facilities or systems as a condition of a contract or provisioning, maintenance, or support of a product or service. SMBs should address such risk prior to granting access. By way of example, access may involve:

1. Access to physical locations housing critical industrial controls or building infrastructure systems (e.g., HVAC, water, power, telecommunications equipment or demarcation, perimeter security, video surveillance, motion detection) or critical information technology/information system (IT/IS) infrastructure (e.g., routers & switches, servers, IT/IS security systems);

2. Logical access to any systems including, but not limited to, those enumerated above, including time-limited access or persistent remote connectivity.

These are provided by way of example and are not intended to be all-inclusive. Access may be time limited based on project requirements or access may be ongoing in order to provide uninterrupted maintenance and support. Regardless of the type or length of access required, the same risks exist and SMBs should address them.

WHAT DECISION OUTCOMES DO THE QUESTIONS SUPPORT?

1. Should we grant or accept access?
    a. Identify: Are there adequate protections in place in my SMB if access to facilities/systems is granted?
    b. Protect: Does my SMB have sufficient personnel security, physical access, logical access controls to protect my business?
    c. Detect: Does my SMB have adequate monitoring to detect when access to facilities/systems is not authorized?
    d. Respond: Does my SMB have sufficient capacity to respond to unauthorized access? Who would need to be notified in the event of a breach?
    e. Recover: Does my SMB have contingency plans in place in the event of disruptive event due to unauthorized access to facilities or systems?

2. Due Diligence -- does the vendor have evidence to show:
    a. Policies and procedures are in place to:
        i. Screen/vet personnel based on their need to have access and personnel access is limited to only the areas necessary to fulfill their specific role.
        ii. Manage physical access control to facilities with cyber assets (network devices, data facilities, patch panels, industrial control systems, programmable logic, etc.).
        iii. Monitor authorizations for separated staff and detect unauthorized access.
    b. Physical security incidents and suspicious events are escalated to cybersecurity operations staff.

c. Security awareness training is provided for logical access? Insider threat protection is provided for the SMB customers' personally identifiable information (PII).

Acquirer Decision Outcome

The SMB is reassured that the managed services provider (MSP) shares its prioritization of supply chain security as a condition for award.

Integrator Decision Outcome

The SMB gains better insight into the MSP's risk profile, which can be used as a tool for evaluating other vendors.

Supplier Decision Outcome

The SMB can demonstrate that the risk management aspect of the business has been well vetted.

Benefits as Acquirer, Integrator, or Supplier

Application of this template will offer many benefits, including:

1. Assist the SMB in assessing potential areas of risk when adding or modifying any product or service(s) to their environment;
2. Help the SMB develop policies, procedures, and mitigations to address risk posture presented by the addition or modification of products or services requiring third-party access;
3. Provide the SMB and potential vendors performance indicators to measure service level agreements or negotiate contractual agreements;
4. Build a decision matrix for the SMB regarding the creation of requests for proposal and selection of products and services; and
5. Provide the SMB a methodology to achieve regulatory or industry compliance(s); e.g., PCI/DSS, ISO 27001, NIST 800-53, etc.

VENDOR TEMPLATE REFERENCES (ACQUIRER, INTEGRATOR, SUPPLIER)

To assist your organization, the following questions apply to most SMBs and to all roles in the supply chain: Acquirer, Integrator, or Supplier. These are not meant to be all-inclusive; rather, they are representative of basic supply chain risk management practices. The complete Vendor Template is available at https://www.cisa.gov/publication/ict-scrm-task-force-vendor-template.

Threshold Questions

If you can provide affirmative responses to the questions below AND supporting, non-expired documentation, you may skip ALL remaining questions.

1.1 Have you previously provided supply chain risk management information to this organization?

If "Yes," please provide an updated revision covering material changes.

> If an SMB is using multiple use cases, it may be helpful to identify common questions among them. Answers to the questions might rest somewhere between "yes" and "no."

OR

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

If you responded affirmatively to ANY of the questions above, you may attach supporting documentation and skip the remaining questions.

Secure Design and Engineering

3.17 Does your organization analyze vulnerabilities to identify root cause?

Information Security

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

4.7 Do you have a regularly maintained asset management program approved by management for your IT assets?

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

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

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

4.17 Do you include contractual obligations to protect information and information systems handled by your suppliers?

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

4.21 Do you have defined and documented incident detection practices?

4.25 Do you have a documented incident response process and a dedicated incident response team?

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

Physical Security

5.2 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.)?

5.3 Do you have documented policies addressing staff training, which includes procedures to limit physical access to cyber assets (network devices, data facilities, patch panels, industrial control systems, programmable logic, etc.) to only those with demonstrated need?

5.4 Do you have a documented Security Incident Response process to address potential or suspected physical security incidents (e.g., potential intruder access, missing equipment, etc.)?

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

Personnel Security

6.2 Do you have a process for onboarding personnel?

6.3 Do you have policies for conducting background checks of your employees?

6.6 Do you have a process for offboarding personnel?

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

6.11 Is there additional security training provided to users with elevated privileges (users)?

EXAMPLE OF VULNERABILITY AND METHODS OF SECURING PHYSICAL AND LOGICAL ACCESS: CASINO HACKED THROUGH FISH TANK THERMOMETER[vi, vii]

In 2017, a casino added a seemingly simple "smart" device – an Internet-connected fish tank thermometer. Cyber criminals then compromised the thermometer, gained a persistent foothold into the casino's network, and were able to exfiltrate data from a database of high-roller gamblers. It is tempting to apportion blame for this breach as failures by the manufacturer, cloud service provider, and the casino's IT/Security staff; however, this is an excellent cautionary tale for every part of a supply chain interaction.

For the Purchaser/Acquirer

- Ask about the manufacturer's software/firmware patches and updates cycles. Are best practices followed to ensure the patches/updates cannot be compromised? Patches and updates should be timely, well documented, and reference lists of common vulnerabilities and exposures ("CVE"), if appropriate.
- The manufacturer should provide sufficient technical documentation or support to ensure a secure deployment in your environment.
- Ensure that your policies and procedures support internal IT/Security standard cybersecurity practices and hygiene for Internet of Things (IoT) or industrial control devices; e.g., network segmentation, changing default credentials or ports, and monitoring and alerting for anomalous traffic.
- Internal IT/Security staff should harden physical and logical access to critical system and privileged accounts; e.g., audited physical access, least privilege principle, and monitoring and regular auditing of privileged accounts/access.
- Update your incident response plan to include the new systems. Make sure that the manufacturer is obligated to assist in incident response during a cyber attack involving their product(s).

[vi] https://money.cnn.com/2017/07/19/technology/fish-tank-hack-darktrace/index.html

[vii] https://thehackernews.com/2018/04/iot-hacking-thermometer.html

For the Integrator

- Follow the same recommendations for the Purchaser/Acquirer.
- Develop standards for deploying the product(s) securely in all practical use scenarios.
- Diversify acquisition to include products of similar operation to protect against supply chain failure or product security breaches.
- Provide Purchaser with a detailed project scoping document.
- Provide Purchaser with technical support in partnership with the Supplier.

For the Supplier/Manufacturer

- Practice secure software development cycles for the product software/firmware. Make certain that external product testing occurs periodically and operate a bug bounty program.
- Vet hardware assemblies for security, including I/O modules and processors.
- Practice standard cybersecurity hygiene for cloud or web-based connectivity to the product(s). Perform periodic testing using OWASP standards.

USE CASE 2

APPLYING VENDOR SCRM TO CLOUD-HOSTED SOLUTIONS

Description

This use case is for those considering the use of cloud-hosted solutions between the small or medium-sized business (SMB) and the company hosting the cloud services that are key to business operations (e.g., business collaboration productivity suites, customer relationship management tools, credit card processing).

For example, this could be necessary if a service provider is outsourcing aspects of customer support of their managed router service – such as Wi-Fi passwords, security, parental controls, etc. – to a cloud provider. As another example, an SMB might outsource marketing to a cloud vendor, and would upload customer PII (e.g., names, addresses, phone numbers) to the vendor on a regular basis. In both cases, the SMB can transfer some risk to the cloud vendors, but the SMB must do its due diligence when selecting those vendors. Selecting a vendor without applying the appropriate vendor SCRM controls could place customers' information at risk and ultimately cause material damage to the SMB. It is critical that the SMB ask the right questions when preparing to enter these relationships.

WHAT DECISION OUTCOMES DO THE QUESTIONS SUPPORT?

This use case is primarily relevant to the following groups:

- Acquirer – An Acquirer that considers ICT supply chain security as part of their selection process.
- Integrator – An SMB providing integration services who needs to articulate and demonstrate appropriate due diligence of the ICT SCRM posture of solutions they are selecting or implementing on behalf of their clients.

Acquirer Decision Outcomes

An Acquirer will use these questions to weigh the risk among multiple cloud-solution providers to ensure the acquirer is fully aware or, accounts for, and manage the risk environment for each potential solution.

Integrator Decision Outcomes

An Integrator will use these questions to better understand, account for, and reduce the risk of providing solutions to one or more customers.

Acquirer Benefits

1. Ensures SMB is aware of SCRM policies and practices in place for vendors of potential solutions
2. May illuminate gaps in the SCRM practices of the potential vendor that the SMB was unaware of previously; may prevent future SCRM issues
3. Ensures SMB accounts for SCRM issues of concern that may be relevant to obtaining government contracts
4. Provides visibility about supply chain risk that can be used for risk sharing, including in contracts

Integrator Benefits

1. Communicates integrator's vendor SCRM commitment to potential customers
2. Ensures consistency in evaluating potential solutions for use by the SMB
3. Demonstrates to SMB that integrator is well-informed on SCRM
4. Provides information to SMB that may be needed quickly in case of an incident
5. Provides visibility about supply chain risk that can be used for risk sharing, including in contracts

VENDOR TEMPLATE REFERENCES (ACQUIRER, INTEGRATOR)

To assist your organization, the following questions apply to most SMBs and to all roles in the supply chain: Acquirer, Integrator, or Supplier. These are not meant to be all-inclusive; rather, they are representative of basic supply chain risk management practices. The complete Vendor Template is available at https://www.cisa.gov/publication/ict-scrm-task-force-vendor-template.

Acquirer Template

<u>Threshold Questions</u>

If an SMB is using multiple use cases, it may be helpful to identify common questions among them. Answers to the questions might rest somewhere between "yes" and "no."

If you can provide affirmative responses to the questions below AND supporting, non-expired documentation, you may skip ALL remaining questions.

1.1 Have you previously provided supply chain risk management information to this organization?

If "Yes," please provide an updated revision covering material changes.

<u>OR</u>

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

If you responded affirmatively to ANY of the questions above, you may attach supporting documentation and skip the remaining questions.

Supply Chain Management and Supplier Governance

2.3 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)?

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

2.5 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?

2.6 For hardware components included in the product offering, do you only buy from original equipment manufacturers or licensed resellers?

2.8. Do you have written Supply Chain Risk Management (SCRM) requirements in your contracts with your suppliers?

Secure Design and Engineering

3.4. Does your organization document and communicate security control requirements for your hardware, software, or solution offering?

3.8. How does your organization prevent malicious and/or counterfeit IP components within your product offering or solution?

3.11. Does your organization verify that third-party software provides required security requirements/controls?

3.15. Does your organization configure offerings to implement secure settings by default?

3.16. Does your organization maintain and manage a Product Security Incident Reporting and Response program (PSRT)?

Information Security

4.1. 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.)? [If yes, please state the program and date that you were certified and provide a copy of the certification. You may skip the remaining questions of this section and proceed to the following section. If no, continue.]

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

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

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

4.6. 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?

4.7. Do you have an asset management program approved by management for your IT assets that is regularly maintained?

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

4.11. Do you have documented policies or procedures for identification and detection of cyber threats?

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

4.16. Is cybersecurity training required for personnel who have administrative rights to your enterprise computing resources?

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

4.21. 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?

4.22. Do you require vulnerability scanning of software running within your enterprise prior to acceptance?

4.23. Do you deploy anti-malware software?

4.24. Do you have a documented incident response process and a dedicated incident response team?

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

Physical Security

5.2 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.)?

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

Personnel Security

6.1. Does a formal personnel security program exist?

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

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

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

6.8. Are Personnel Security practices routinely enforced, audited, and updated?

6.13. Do you have a Code of Conduct for your employees, suppliers and subcontractors?

Supply Chain Integrity

7.5. Do you monitor third-party HW/SW products or services for defects?

7.8. Do you have processes to evaluate prospective third-party suppliers' product integrity during initial selection?

Integrator Template

Threshold Questions

If you can provide affirmative responses to the questions below AND supporting, non-expired documentation, you may skip ALL remaining questions.

1.1. Have you previously provided supply chain risk management information to this organization?

If "Yes," please provide an updated revision covering material changes.

> If an SMB is using multiple use cases, it may be helpful to identify common questions among them. Answers to the questions might rest somewhere between "yes" and "no."

OR

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

If you responded affirmatively to ANY of the questions above, you may attach supporting documentation and skip the remaining questions.

Supply Chain Management and Supplier Governance

2.1 Do you have policies to ensure timely notification of updated risk management information previously provided to us?

2.3 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)?

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

2.5 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?

2.6 For hardware components included in the product offering, do you only buy from original equipment manufacturers or licensed resellers?

2.8. Do you have written Supply Chain Risk Management (SCRM) requirements in your contracts with your suppliers?

Secure Design and Engineering

3.4. Does your organization document and communicate security control requirements for your hardware, software, or solution offering?

3.6. Does your organization protect all forms of code from unauthorized access and tampering, including patch updates?

3.7. Does your organization provide a mechanism for verifying software release integrity, including patch updates for your software product offering?

3.8. How does your organization prevent malicious and/or counterfeit IP components within your product offering or solution?

3.10. Does your organization define, follow, and validate secure coding and manufacturing practices to mitigate security risks?

3.11. Does your organization verify that third-party software provides required security requirements/controls?

3.15. Does your organization configure offerings to implement secure settings by default?

3.16. Does your organization maintain and manage a Product Security Incident Reporting and Response program (PSRT)?

Information Security

4.1. 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.)?

[If yes, please state the program and date that you were certified and provide a copy of the certification. You may skip the remaining questions of this section and proceed to the following section. If no, continue.]

4.2. 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)?

4.3. Do you have company-wide, publicly available information security policies in place covering privacy policies?

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

4.6. 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?

4.7. Do you have an asset management program approved by management for your IT assets that is regularly maintained?

4.8. Do you have documented policies or procedures to manage enterprise network-connectable assets throughout their lifecycle?

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

4.10. Do you have documented hardware and software policies and practices in place to ensure asset integrity?

4.11. Do you have documented policies or procedures for identification and detection of cyber threats?

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

4.16. Is cybersecurity training required for personnel who have administrative rights to your enterprise computing resources?

4.17. Do you include contractual obligations to protect information and information systems handled by your suppliers?

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

4.21. 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?

4.22. Do you require vulnerability scanning of software running within your enterprise prior to acceptance?

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

4.24. Do you deploy anti-malware software?

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

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

Physical Security

5.2. 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.)?

5.3. Do you have documented policies addressing staff training which includes procedures to limit physical access to cyber assets to only those with demonstrated need?

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

5.5. For facilities that use an independent contractor for physical security, are physical facilities' security policies and procedures incorporated into service level agreements, contracts, policies, regulatory practices?

5.10. Do you have processes in place to prevent counterfeit parts from entering your supply chain?

Personnel Security

6.1. Does a formal personnel security program exist?

6.2 Do you have processes for onboarding personnel?

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

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

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

6.6. Do you have a process for offboarding personnel?

6.8. Are Personnel Security practices routinely enforced, audited, and updated?

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

6.11. Is there additional security training provided to users with elevated privileges?

6.13. Do you have a Code of Conduct for your employees, suppliers, and subcontractors?

Supply Chain Integrity

7.3. Do you have documented performance and validation procedures for your HW/SW products or services?

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

7.5. Do you monitor third-party HW/SW products or services for defects?

7.8. Do you have processes to evaluate prospective third-party suppliers' product integrity during initial selection?

Supply Chain Resilience

8.3. Do you maintain a formal business continuity plan necessary to maintain operations through disruptions and significant loss of staff?

8.5. Can personnel work remotely?

EXAMPLE OF VULNERABILITY RELATIVE TO CLOUD SERVICE PROVIDERS[viii, ix]

In 2021, a group of threat actors announced that they had breached a cloud-based security camera vendor. Threat actors claimed to have gained access to 150,000 surveillance cameras inside police departments, prisons, schools, hospitals, and private organizations. The breach impacted well-known firms, allowing threat actors access to live feeds in a number of sensitive areas.

USE CASE 3

VETTING MANAGED SERVICE PROVIDERS (MSPs)

Description

The goal is to create a template to help SMBs vet Managed Service Providers (i.e., vendors that will have "critical access" [root, superuser, admin] to their systems or data).

The use case for this template is the selection of a managed service provider (MSP) to provide technical assistance to a small or medium-sized business (SMB). The SMB has a contract with a large client that is very particular about Supply Chain Risk Management, and the contract calls upon the SMB to manage down-stream supply chain risks introduced by vendors that have "critical access" to systems or data. Because the MSP will be installing and managing hardware and software systems, it requires giving the MSP "critical access" (root, superuser, admin) to their systems or data. Therefore, the MSP falls within the scope of the contractual agreement with respect to managing supply chain risk.

[viii] https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams
[ix] https://www.cyberscoop.com/verkada-breach-surveillance-facial-recognition-privacy/

WHAT DECISION OUTCOMES DO THE QUESTIONS SUPPORT?

This use case is primarily relevant to the following groups:

- Acquirer - An Acquirer that considers ICT supply chain security as part of their selection process.

Acquirer Decision Outcomes

1. The SMB is reassured that the MSP shares its prioritization of supply chain security as a condition for awarding the master service contract.
2. The SMB can demonstrate to management that with respect to at least overall enterprise risk management, this particular aspect of the business has been well vetted.
3. The SMB gains better insight into the MSP's risk profile for current contract, as well as for comparison with other MSPs in future Request for Proposal (RFP) endeavors.

Acquirer Benefits

1. Reassures its directors, investors, and insurers that it has taken all steps to ensure the provenance of component inputs in its final service.
2. Provides added credibility to Acquirer's status in industry.
3. Provides added level of security and trust in the vendor's services.
4. Enhances current and potential future quality of vendor-acquirer relationship.
5. Enhances process transparency

VENDOR TEMPLATE REFERENCES (ACQUIRER)

To assist your organization, the following questions apply to most SMBs and to all roles in the supply chain: Acquirer, Integrator, or Supplier. These are not meant to be all-inclusive; rather, they are representative of basic supply chain risk management practices. The complete Vendor Template is available at https://www.cisa.gov/publication/ict-scrm-task-force-vendor-template.

Acquirer Template

Threshold Questions

If you can provide affirmative responses to the questions below AND supporting, non-expired documentation, you may skip ALL remaining questions.

1.1. Have you previously provided supply chain risk management information to this organization?

If an SMB is using multiple use cases, it may be helpful to identify common questions among them. Answers to the questions might rest somewhere between "yes" and "no."

If "Yes," please provide an updated revision covering material changes.

OR

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

If you responded affirmatively to ANY of the questions above, you may attach supporting documentation and skip the remaining questions.

Supply Chain Management and Supplier Governance

2.1. Do you have policies to ensure timely notification of updated risk management information previously provided to us?

2.3. 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)?

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

2.7. Do you have a process for tracking and tracing your product while in development and manufacturing?

2.8. Do you have written Supply Chain Risk Management (SCRM) requirements in your contracts with your suppliers?

2.9. Do you revise your written SCRM requirements regularly to include needed provisions?

2.10. 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)?

Secure Design and Engineering

3.4. Does your organization document and communicate security control requirements for your hardware, software, or solution offering?

3.7. Does your organization provide a mechanism for verifying software release integrity, including patch updates for your software product offering?

3.8. How does your organization prevent malicious and/or counterfeit IP components within your product offering or solution?

3.11 Does your organization verify that third-party software provides required security requirements/controls?

3.14. Does your organization implement formal vulnerability and weakness analysis practices?

3.16. Does your organization maintain and manage a Product Security Incident Reporting and Response program (PSRT)?

Asset Management

4.6 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?

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

4.11. Do you have documented policies or procedures for identification and detection of cyber threats?

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

4.16. Is cybersecurity training required for personnel who have administrative rights to your enterprise computing resources?

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

4.24. Do you deploy anti-malware software?

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

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

Physical Security

5.2. 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.)?

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

5.7. 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.

Personnel Security Questions

6.1. Does a formal personnel security program exist?

6.6. Do you have a process for offboarding personnel?

6.7. Are personnel security practices formally documented and accessible to all employees?

6.8. Are Personnel Security practices routinely enforced, audited, and updated?

6.9. Are personnel required to complete formal SCRM training annually?

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

6.11. Is there additional security training provided to users with elevated privileges?

6.12. Are you aware of security training practices performed by your sub-suppliers to their personnel?

Supply Chain Integrity

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

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

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

7.6. Does the functional integrity of your product or services rely on cloud services (commercial or hybrid)?

7.8. Do you have processes to evaluate prospective third-party suppliers' product integrity during initial selection?

7.9. Do you have regularly scheduled audits to ensure compliance with HW/SW products or services integrity requirements?

Supply Chain Resilience

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

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

8.3. Do you maintain a formal business continuity plan necessary to maintain operations through disruptions and significant loss of staff?

8.4. 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?

8.6. 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?

EXAMPLE OF VULNERABILITY RELATIVE TO MANAGED SERVICE PROVIDERS[x,xi]

In 2013 a group of threat actors compromised at least 40 million credit and debit card accounts belonging to consumers who shopped at a number of the same store locations. The threat actors gained access to the store's internal networks via a vendor portal by compromising login credentials from a refrigeration contractor. These stolen login credentials allowed the threat actor to gain trusted access to the store's network and exfiltrate data.

[x] https://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/
[xi] https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

APPENDIX A: CASE STUDY FOR VETTING A MANAGED SERVICE PROVIDER

For years now, various operational tools that businesses rely upon have been migrating toward a subscription model and away from outright ownership by the business. Common business software such as Microsoft Word, Excel, and PowerPoint are now only available on a subscription basis. Intuit is heavily marketing QuickBooks online as the alternative to its desktop versions and incentivizing switching with promotions and improved functionality. Even a business's physical security investments are switching from a CapEx to an OpEx model by leveraging offers from companies providing video surveillance and access control as a service enabled via advancements in the technology and adoption of cloud services.

The financial benefits of these new service models for small and medium-sized businesses are real, especially in their ability to better align and correlate a business's expenses and revenues for improved cash flow. They also allow the business to realize improvements in productivity and efficiency immediately without having to fund large capital injections that used to be needed. However, these services can create cyber vulnerabilities that SMBs need to review and mitigate. This framework can be used to vet services offerings just as effectively as it can for traditional capital expenses.

In this example, an SMB is looking to install a physical security system in their office facilities. Physical security measures are important for protecting staff and property from unwanted intrusion. In a competitive environment, physical security measures can also help to protect and safeguard a business's intellectual property and position an SMB as a trusted supplier to its downstream customers, especially if those customers are direct or indirect contractors to government entities.

Physical security offerings available today include on-premises equipment sold thru distributors and Value-Added Resellers (VARs) as well as subscription models where equipment and management software are delivered in exchange for a monthly or annual subscription fee. In this example, the Working Group will look specifically at the subscription model for a video surveillance system.

Video surveillance systems consist of cameras mounted throughout a facility (exterior and interior), storage for the video footage, and software used for search and retrieval of that footage. In most subscription models, the cameras transmit their footage to cloud-hosted storage with a software client capable of managing the health of the cameras, searching and retrieving stored footage, and processing alarms. SMBs that use these services forego the upfront cost for the equipment and installation labor, as well as the on-going costs of maintaining storage servers and the nuisance of software patches. However, in doing so, they accept the notion that footage of their facility and people will be stored somewhere in a public cloud, trusting the vendor's security measures to ensure proper confidentiality. Examples of how the framework can be used to vet potential suppliers is presented in the next section.

VENDOR TEMPLATE REFERENCES (ACQUIRER)

2.3. *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)?*

(Video surveillance services typically rely on public cloud infrastructures. It is important to understand where the information from your facility is physically stored, for how long, and who has access to the data as vulnerabilities and attacks upon these platforms can impact your business's cyber risk profile.)

[Yes, No, Alternate, or N/A]

Appropriate responses: Yes or Alternative. A suitable supplier would ideally have processes and procedures in place to ensure the provenance of system components and to control the chain of custody of components throughout their life cycle, including proper retirement and disposal of said components.

2.3.1. *What is your strategy?*

Appropriate responses: A suitable supplier would at a minimum have a strategy in place that comports with industry best practices and established guidelines for managing supply chain risks, such as those outlines by CISA and NIST. A Supplier should affirm that it adheres to the principles outlined in CISA's IT Managed Services Risk Framework.

2.3.2. *How have you implemented it?*

Appropriate responses: A suitable supplier would be able to demonstrate how the process is implemented within the organization, including regular training and staff education.

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

(Government sanctions [for example, the NDAA of 2018] stipulate certain commercial entities that cannot be used on government networks or by government contractors. As equipment supplied in surveillance services may be bundled together with the service and not purchased separately, it is important to ensure they do not come from sanctioned entities.)

Appropriate responses: Yes. A suitable organization would have at least an awareness of prohibited telecommunications services and equipment pursuant to the 2019 NDAA (The John S. McCain National Defense Authorization Act for Fiscal Year 2019) and actions related thereto by the Department of Commerce and the Federal Communications Commission. Similarly, the supplier should have awareness of Department of Energy actions regarding supervisory control and data acquisition (SCADA) and industrial control systems for controlled or banned hardware.

2.7. *Do you have a process for tracking and tracing your product while in development and manufacturing?*

[Yes, No, Alternate, or N/A]

Appropriate responses: Yes or Alternative. A suitable supplier would have situational awareness of the production and parts sourcing of its downstream manufacturers, including a knowledgeable awareness of the development process.

2.7.1. *How do you keep track of your chain of custody?*

Appropriate responses: An appropriate response would demonstrate having established a close working relationship with component part manufacturers, which in turn would be coupled with visibility into those suppliers' processes to ensure the provenance of component parts as well as the integrity of those components from assembly, packing, and distribution or delivery.

2.7.2. *How do you track and trace components within your product?*

Appropriate responses: A suitable supplier should have the ability to track and trace each component that comprises its product—from suppliers and manufacturers through assembly and final delivery to customers. Traceability is “the ability to trace the history, application or location of an entity by means of recorded identifications.”[xii] Specifically, the supplier should use bar codes and RFID as standard practice. Ideally the process employed should be automatic, with the ability to correlate various data on the component as it moves through the supply/delivery chains.

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

(One of the benefits of using cloud-based software instead of purchasing software is that updates can be made automatically and globally by the vendors themselves. Understanding that vendor’s frequency of patch releases, service level agreements [SLAs] around time of vulnerability identification to patch release, etc. would be important.)

Appropriate responses: Yes or Alternative. A suitable supplier should be able to point to the organization’s coding standards; that is, a collection of coding rules, guidelines, and best practices that help it to ensure that the software in question is safe, secure, and reliable. The supplier should also be able to point to internal initiatives it has taken to educate appropriate key staff on what those coding standards are and how to best implement them.

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

Appropriate responses: Yes or Alternative. Similar to above, a suitable supplier should have a process in place that employs some form of component traceability to protect their production lines (including downstream suppliers) from the threat of the counterfeit components or parts. This is a supply chain integrity and cybersecurity issue, as well as a basic quality control issue. The supplier should be aware of blacklist component suppliers. The organization should have training in place to educate staff on identifying and testing for malicious or counterfeit IP components. The organization would ideally have a zero tolerance policy for counterfeits by ensuring that they use only authorized supply channels.

3.11. *Does your organization verify that third-party software provides required security requirements/controls?*

Appropriate responses: Yes.

3.14. *Does your organization implement formal vulnerability and weakness analysis practices?*

Appropriate responses: Yes or Alternative.

3.16. *Does your organization maintain and manage a Product Security Incident Reporting and Response program (PSRT)?*

Appropriate responses: Yes or Alternative.

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

(Unfortunately, most data breaches go unnoticed by the victim network until a customer or third-party entity notifies the owners. It is not uncommon for a breach to go undetected for six or more months before a notification is received and evidence of the breach is researched. Maintaining open

[xii] EN ISO 8402 (1994) Quality Management and Quality Assurance - Vocabulary

channels of communication with vendors in your supply chain can help expedite the notifications and allow you to take proper action to remediate the vulnerability and mitigate the potential damage.)

Appropriate responses: Yes or Alternative

4.11.1. *What processes do you have in place to promptly detect cyber threats?*

Appropriate responses can include having internal security assessment teams routinely audit a company's software. A company could also subscribe to a public information forum (such as CISA) for threat updates and process notifications by checking their software build libraries and scanning to ensure patches are properly applied.

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

Appropriate response can include having contractual arrangements with software suppliers whereby suppliers are required to notify the small/medium-sized business upon a breach, or an SLA that clearly states how long before a supplier is required to publish a security patch after a vulnerability is made public.

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

Appropriate responses can include reviewing all public domain alerts of known vulnerabilities and publishing a statement as to whether the vulnerability impacts a supplier's product.

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

Appropriate responses: Yes or Alternative

4.15.1. *If "Yes," please list any standards or frameworks used?*

Appropriate responses can include following NIST guidelines and frameworks or using an updated network vulnerability scan tool to routinely scan for known vulnerabilities.

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

Appropriate responses can include using access control lists (ACLs) to manage who has access to vital systems; deploying network monitoring tools to detect if and when a privilege is elevated.

4.15.2.1. *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.)?*

Appropriate responses can include the use of VPNs to secure all remote access to the supplier's network, as well as logging all non-employee access by third parties to the company's network assets and deactivating those connections once the task has been completed.

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

Appropriate responses can include running network scans to identify unknown MAC addresses, having policies in place around BYOD (Bring Your Own Device) security, or having segmented networks to protect access and rights to critical servers and computing devices.

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

Appropriate response is Yes. Be wary of suppliers that respond in the negative.

4.16.1. *What is the frequency for verifying personnel training compliance?*

Appropriate responses would include a timeframe of how frequently personnel must complete this training, how frequently the training is updated, and how the organization enforces compliance.

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

Appropriate answers can include separating third parties and guests to only accessing a guest network or permitting access only to needed systems on the main network with basic privileges.

4.16.2.1. *How is training compliance tracked for third parties with network access?*

(During a recent, well-publicized breach of a cloud/video provider, it was determined that several employees of the breached company had super-admin access rights to systems sold and installed at customer sites without customers knowing about it.)[xiii]

Appropriate response includes confirmation of multiple tools to track employee adherence, and completion of cyber training.

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

Appropriate response: Yes or Alternative (Alternative is acceptable only if the vendor uses a third party or external MSP to manage their network and software patches.)

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

Appropriate answers can include deploying patches and updates using a central network management tool. Look for indications of a management capability to detect the version of software running on different devices and enforce network rules against those found to not have been patched. A significant number of breaches occur when one system or server has not been updated to the latest security patch, leaving a vulnerability for an attacker to leverage.

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

Appropriate responses: Yes or Alternative. The vendor should include details of business continuity

[xiii] https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams

systems and plans, including automatic backups of critical databases and servers.

4.26.1. *What is the frequency for testing of back-up media?*

Appropriate responses can include weekly or monthly frequencies.

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

(While cyber-attack insurance is available, adoption is still not as widespread. Regulations in certain jurisdictions (and especially in Europe) are designed to protect a business's customers should the business be a victim of a cyber-attack. These regulations hold the business accountable for damage incurred by the theft of personal identification information of that business's customers. Look for vendors that understand the risks your business can face and either have exposure to the same regulations or have insurance to cover your damages should the breach come thru their product offer.)

Appropriate responses: Yes or Alternative.

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

Appropriate responses: Ideally, yes or alternative, but the response to this question may depend on whether particular insurance instrument includes provisions for customer coverage that is not required as a widely-accepted best practice standard for cybersecurity.

6.1. *Does a formal personnel security program exist?*

Appropriate response: Yes. A company providing video surveillance equipment and services should be able and willing to provide details of its formal personnel security program to the SMB. An SMB acquiring such equipment and services should not put its own operations at risk by using a company without a formal personnel security program.

6.1.1. *Is employee access managed by role?*

Appropriate response: Yes. Managing access by roles is a standard good practice enabling least privilege access. A negative response can indicate the company providing equipment and services to the SMB is unable to adequately identify, manage, and limit access to individuals appropriately.

6.1.2. *Is access to business-critical systems, manufacturing facilities, and assets formally managed and maintained? Please describe.*

Appropriate response: Yes. It is essential that a company providing video surveillance equipment and services to an SMB formally manages and maintains access to business-critical systems, facilities, and assets. If a provider of video surveillance equipment and services does not formally manage and maintain access to their business-critical systems, facilities, and assets, an SMB that contracts with or subscribes for that company's equipment and services puts itself and its own operations at substantial risk from hackers or that company's own insider threats.

6.6. *Do you have a process for offboarding personnel?*

Appropriate response: Yes. Our on- and off-boarding process is co-managed between our HR and IT departments. Our IT department uses an IT Asset Management system that maps assets and accounts to employees. A company providing video surveillance equipment and services should be able and willing to provide details of its personnel offboarding process to the SMB. SMB acquiring such equipment and services should not put its own operations at risk by using a company without a process for offboarding personnel.

> 6.6.2. *What is the process to remove access to all company documents, applications, assets, etc.?*
>
> Appropriate response: Our personnel offboarding process requires termination of all access to company documents, systems, applications, and accounts no later than 5:00 pm (local time) on the employee's final day of employment. The employee and that employee's supervisor are responsible for notifying our IT department of an employee's last day not later than 72 hours prior, or immediately when 72-hour advance notice is not practicable.
>
> 6.6.3. *What is the process to recover all company assets?*
>
> Appropriate response: Employees are accountable for company assets issued to them with hand receipts maintained by our IT department using the asset management system. When notified of an employee's termination, the IT department schedules an appointment with the employee to return company assets. If the employee does not return the assets when scheduled, our IT department will immediately revoke all employee access to systems, networks and accounts. We then inform the employee and supervisor. If an in-house employee does not return company assets prior to the end of their last day, or by mail within 7 days for telework employees, the company takes progressively stronger actions (up to and potentially including legal action).

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

Appropriate response: Yes. We have an extensive training protocol for all employees. Security training is required of all new employees and is required as refresher training for all employees annually.

6.11. *Is there additional security training provided to users with elevated privileges?*

Appropriate response: Yes. Absolutely. Additional security training is required as an essential part of our Privileged Access Management program. This is training is required for individuals to obtain and maintain access to privileged accounts.

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

Appropriate response: Yes or no are acceptable responses. The key point is that the company knows the components and their provenance of their product or service.

> 7.6.1. *What policies and procedures are in place to protect the integrity of the data provided through cloud services?*
>
> Appropriate response: When selecting a cloud service provider, we vetted companies on whether they segmented virtual machine networks for different customers. Internally, we

protect our customers’ data through applying security software (including antivirus), patch maintenance, minimizing privileges, and encrypting communications.

APPENDIX B: REFERENCES

CYBER ESSENTIALS[1]

- CISA's Cyber Essentials is a guide for leaders of small businesses as well as leaders of small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices.

CYBER ESSENTIALS STARTER KIT[2]

- The Cyber Essentials Starter Kit is a set of modules that leaders and their staff can use as a starting place for building a culture of cyber readiness consistent with the NIST cybersecurity framework and other standards.

CYBERSECURITY RESOURCES ROAD MAP[3]

- The Cybersecurity Resources Road Map is designed to help critical infrastructure small and midsize businesses identify useful cybersecurity resources to meet their needs.

HEALTH INDUSTRY CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT GUIDE (HIC-SCRIM)[4]

- The Healthcare and Public Health Sector Coordinating Council (HSCC) Joint Cybersecurity Working Group (JCWG) Supply Chain Cybersecurity Task Group developed this supply chain cybersecurity risk management guide to provide structure and aid as a tool targeted at smaller to mid-sized health organizations.

NASA SEWP V TRAINING VIDEO - OPEN TRUSTED TECHNOLOGY PROVIDER STANDARD CERTIFICATION - ISO 20243[5]

- NASA created a training video about ISO 20243, also known as the Open Trusted Technology Provider Standard Certification (O-TTPS), a standard created by The Open Group.

NIST CYBERSECURITY PRACTICE GUIDE SP 1800-15[6]

- SP 1800-15 describes for IoT product developers and implementers four different implementations that use Manufacturer Usage Description (MUD) to automatically limit IoT devices to sending and receiving only the traffic that they require to perform their intended functions.

SECURITY POLICY TEMPLATES[7]

- SANS has developed and posted here a set of security policy templates.

SOLUTIONS FOR ENTERPRISE WIDE PROCUREMENT (SEWP) ISO 20243 (SCRM)[8]

- The ISO 20243, also known as the Open Trusted Technology Provider Standard Certification (O-TTPS), is a standard created by The Open Group.

STOP.THINK.CONNECT[9]

- Stop.Think.Connect is a global online safety awareness campaign that includes resources and materials to help keep your small business cyber secure.

APPENDIX C: QUESTIONS IN ALTERNATIVE FORMAT

EXCEL SPREADSHEET[10]

- The Working Group developed a spreadsheet as an alternate tool, intended to allow options to accommodate yes, no, or partial responses to each of the questions selected in the guide.

DISCLAIMER: This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this report or otherwise. This report is TLP: WHITE: Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see www.cisa.gov/tlp.

DHS POINT OF CONTACT

National Risk Management Center

Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
NRMC@hq.dhs.gov
For more information about NRMC, visit www.cisa.gov/national-risk-management

[1] https://www.cisa.gov/cyber-essentials
[2] https://www.cisa.gov/sites/default/files/publications/Cyber Essentials Starter Kit_03.12.2021_508_0.pdf
[3] https://us-cert.cisa.gov/resources/smb
[4] https://healthsectorcouncil.org/hic-scrim-v2/
[5] https://www.youtube.com/watch?v=dmLEDkXqEkQ
[6] https://csrc.nist.gov/News/2021/mitigating-network-based-attacks-on-iot-devices-us
[7] https://www.sans.org/information-security-policy/
[8] https://www.sewp.nasa.gov/iso_20243.shtml
[9] https://www.cisa.gov/publication/stopthinkconnect-small-business-resources
[10] https://www.cisa.gov/ict-scrm-task-force