Global City Teams Challenge
Cybersecurity and Privacy Advisory Committee

Guidance for Smart Cities and Municipalities
Cyber Supply Chain Risk Management (C-SCRM)

July 10, 2020

Authors:

Carter Schoenberg, CISSP

Dean Skidmore

Karen Jensen

Table of Contents

Abstract

Since 2017, the volume and velocity of cyber-attacks on municipalities has increased significantly. Government enterprises across the United States must have the ability to reduce their exposure to harm stemming from actions associated with business associates and supply chain partners. In 2019 alone, numerous cities across the United States fell victim to ransomware thus rendering core networking functions and even first responder communications inoperable. In May of 2020, the Global City Teams Challenge (GCTC) Cybersecurity and Privacy Advisory Committee released a white paper on ransomware and its impacts of smart cities.[1] This publication provides local and state agencies within the United Sates a set of recommended security requirements to be incorporated into their acquisition strategy, to include, but not limited to, solicitations (Requests for Proposal), Service Level Agreements, and Terms and Conditions.

The United States Department of Homeland Security also published a whitepaper for stakeholders charged with the responsibilities of designing smart cities[2] and touches upon matters of acquisition focusing on factors to be considered "baked in" as essential design strategies to ensure system availability.

The recommended security requirements (recommendations) described in this document apply to all components of nonfederal systems and provide organizations with legal, regulatory and industry compliance guidelines to safeguard sensitive information and to ensure the confidentiality, integrity and availability of mission critical systems designed to support traditional governmental activities. These recommendations are not legal advice but rather an incorporation of suggested methods based on years of evaluating what is consistently missing within legally binding agreements when a cybersecurity crisis event occurs.

Acknowledgements

The authors greatly appreciated the past works led by Ron Ross, Jon Boyens, Katie Arrington, Emile Monette, Don Davidson, Sokwoo Rhee, Joseph Jarzombek, and the members of the Global City Teams Challenge Cybersecurity and Privacy Advisory Committee that formed the foundation of government enterprises collaborating with industry to improve our cyber risk posture.

[1] "A Starting Point for Smart Cities and Communities on Managing Ransomware Risk", GCTC (2020) https://pages.nist.gov/GCTC/uploads/blueprints/2020-CPAC-Ransomware-Resource-May-2020.pdf

[2] "Trust is Smart Cities System Report", DHS (2020) https://www.cisa.gov/sites/default/files/publications/Trust%20in%20Smart%20City%20Systems%20Report_0.pdf

VERSION

Version	Date	Changes Made	Page Number
FINAL 1.0	July 10, 2020	Final Version	

1.0 INTRODUCTION

According to the U.S. Department of Homeland Security (DHS), Cyber Supply Chain Risk Management (C-SCRM) is the process of identifying, assessing, preventing, and mitigating the risks associated with the distributed and interconnected nature of Information and Communications Technology (ICT) (including the Internet of Things) product and service supply chains. C-SCRM covers the entire life cycle of ICT, and encompasses hardware, software, and information assurance, along with traditional supply chain management and supply chain security considerations. In February of 2020, a Threat Evaluation Working Group[3] created threat scenarios predicated upon supply chain risk.

Numerous cyber frameworks and guidance documents exist including National Institute of Standards and Technology (NIST) Special Publication 800-161 "*Supply Chain Risk Management Practices for Federal Information Systems and Organizations*". Identifying those that most closely align to smart city and local government operations is critical for fostering adoption as State and local agencies do not always desire to follow guidance specific to federal systems. As such, recent additions and enhancements to the (NIST) Special Publications 800-53r5 "*Security and Privacy Controls for Information Systems and Organizations*" and 800-171 "*Protecting Controlled Unclassified Information in Non-Federal Systems and Organizations*" are most applicable. Each of these Special Publications include safeguarding controls that apply to supply chain, and in some cases, tailored for privacy related matters as well.

Advancements in technology are benefiting local governments across the United States in ways that could not have been foreseen less than twenty years ago. As future governmental systems that drive towards smart city initiatives, including the use of traffic management systems, speed enforcement cameras, stop light cameras, to the now wide adoption of the Internet of Things (IoT), a common factor exists in the reliance on external technology goods and service providers to help carry out a wide range of missions and business functions using state-of-the-practice information systems.

Many local and state agencies infrastructures rely on a combination of small and medium size business enterprises, as part of Diversity and Inclusion policies and standards, and very large and well-established enterprises like Microsoft, Google, Amazon, etc. In most cases, after a solicitation is released and subsequently awarded to winner, a unique challenge exists. For example, the awardee may routinely process, store, and transmit sensitive information in their systems to support the delivery of essential products and services to the local or state agencies (e.g., technology support, security as a service, credit card processing, email solutions, processing healthcare data, or cloud services). Additionally, Personally Identifiable Information

[3] DHS CISA - Threat Evaluation Working Group: Threat Scenarios (2020)
https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report_0.pdf

(PII) or Protected Health Information (PHI) is frequently shared with numerous State and Local entities.

Reports from Ponemon[4] highlight in 2019, 56% of organizations suffered a breach caused by one of their vendors. This constitutes a 78% increase from 2018. In 2019 alone, over 100 government and educational facilities were compromised. Of notable interest were the City of Atlanta, the City of Baltimore, and over 20 agencies across the State of Texas. [5]

Small and medium size businesses represent the largest percentage of corporate enterprises in the United States that support Local and State governments. It is important to note that 43% of all reported cyber-attacks target small and medium size businesses (SMB)[6]. When these incidents occur, approximately 60% go out of business due to the lack of risk transference to a cyber liability policy. Even when insurance policies are obtained, data from NetDiligence[7] supports that the total costs associated with a cyber incident compared to the cyber policy value is short by over $1,000,000.

Government has historically not evolved as fast as its industry counterpart, and as the dependency on third party support continues to grow, the ability to hold industry accountable to the same minimum requirements of most Fortune 100 companies becomes necessary. This was realized by the U.S. Federal Government as far back as 2013 when President Barrack Obama tasked the General Services Administration and the Department of Defense to codify a future facing program to limit the Government's exposure to harm associated with the unauthorized release or theft of state secrets. This tasking led to the development of the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), updates to the Defense Federal Acquisition Regulations (DFAR), Homeland Security Acquisition Regulation (HSAR), and most recently, the Cybersecurity Maturity Model Certification (CMMC).

Beginning in 2014, two states, Montana and South Carolina, had comprehensive acquisition reform to include contract language that directly holds contract award winners accountable for any system disruption, damage, or unauthorized release of sensitive information that triggers a harm event requiring breach notifications as required under state laws. The requirements included that the contractor possess no less than $2,000,000 in cyber liability insurance that covers first and third-party damages; demonstration of an independent validation and verification of the contractor's internal cybersecurity operating practices; and annual cybersecurity and privacy training.

---

[4] "5 Reasons Why Supply Chain Security Must be on your Radar", Venture Beat Magazine (2020). https://venturebeat.com/2020/01/08/5-reasons-why-supply-chain-security-must-be-on-your-agenda/

[5] "8 Cities that have been crippled by cyber-attacks", Business Insider (2020). https://www.businessinsider.com/cyberattacks-on-american-cities-responses-2020-1

[6] Overview: 30 Small Business Cyber Security Statistics, Fundera (2020). https://www.fundera.com/resources/small-business-cyber-security-statistics

[7] Cyber Liability Study, NetDiligence (2019) https://netdiligence.com/wp-content/uploads/2018/11/2018-NetDiligence-Claims-Study_Version-1.0.pdf

1.1 Purpose and Target Audience

Disclaimer:

This document focuses on identifying best practices smart city acquisition professionals can use to dramatically reduce key areas of risk. It is not intended to endorse or renounce any commercial products or services, specific organizations, or any particular approach, implementation, or solution for addressing the very complex task of supply chain risk management. The basis of the recommended safeguards is predicated upon numerous cyber and privacy risk assessments of public and private sector enterprises, including supply chain business associates. This document is not meant to be construed as legal guidance.

When addressing cyber supply chain risk management risk, Smart Cities and Municipalities should identify the risk management processes and associated products, services, and solutions that best fit your environment and requirements.

The challenges and concerns identified by industry are also supported by the United States Government. Earlier in 2020, the Cybersecurity and Infrastructure Security Agency (CISA) released a report[8] providing details about the unique threats that are applicable to the acquisition of IoT devices.

This publication is intended to serve a diverse group of individuals and organizations in the public sector including, but not limited to:

- Individuals with acquisition or procurement responsibilities (e.g., contracting officers)
- Individuals with system, security, or risk management and oversight responsibilities (e.g., authorizing officials, chief information officers, chief information security officers, system owners, information security managers)

2.0 SUGGESTED REQUIREMENTS FOR THE SUPPLY CHAIN

2.1 Technology Goods

For the purpose of this document, technology goods are defined as hardware, software, firmware, IoT devices, networking infrastructure (wired and wireless), commercial off-the-shelf (COTS) products and cloud services environments, including infrastructure/hardware as a service (IaaS/HaaS), software as a service (SaaS), and platform as a service (PaaS).

[8] Internet of Things Security Acquisition Guidance (2020)
https://www.cisa.gov/sites/default/files/publications/20_0204_cisa_sed_internet_of_things_acquisition_guidance_final_508_0.pdf

2.2 Technology Services

For the purpose of this document, technology services are defined as professional and/or managed services where a third party has access to, is responsible for the management of, or has personnel accessing information technology/systems belonging to a government entity.

Below are example requirements from NIST Special Publication 800-171 Rev. 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*.

3.0 WHAT SMART CITIES AND AGENCIES SHOULD LOOK FOR

The risks associated with supply chain risk management are not new. A number of commercial enterprises have developed algorithms to identify the alleged "cyber hygiene" of other businesses and creating a cyber score in some ways consistent with a traditional consumer credit score or rating by Duns and Bradstreet. While these models are currently utilized by insurance underwriter as part of their due diligence for policy coverages and premium determination, these "scores" cannot see within the organization and this document acts as an operational guidance document that enables smart cities and other municipal government entities to properly identify potential threats and limit the exposure of a risk by means of contractual enhancements.

3.1 ACCESS CONTROLS

Government enterprises cannot presume that vendors, even security vendors, have adopted industry accepted best practices or commercially reasonable cybersecurity. An example of a best practice is the Cybersecurity Maturity Model Certification (CMMC) was an evolution of NIST Special Publication 800-171, *Protecting Controlled Unclassified Information (CUI) in Non-Federal Systems and Organizations*, which did not require policies and procedures for safeguarding systems and sensitive information. CMMC[9] levels that include CUI (Level 3 and higher) now must demonstrate operational practices that include corporate policies to ensure the enforcement of access control best practices.

A core competency in any mature cyber and privacy risk practice is knowing what is on your network. *You cannot protect what you do not know* is one of the oldest cybersecurity maxims.

[9] CMMC Accreditation Body, 2020. https://www.cmmcab.org/

However, many small and medium size businesses (SMBs) do not have the technical capability or in-house staff to foster the adoption of these practices.

It is incumbent upon the State or local government agency to understand how these challenges may pose a risk. The acquisition workforce cannot and should not be expected to be cyber and privacy liability specialists; however, the safeguarding best practices described in this document provides a variety of things to consider.

3.1.1 Account Management – How does the vendor limit access to their information systems to only authorized users?

1. Does the vendor have a network protected from the Internet by a firewall and if so, what kind?

   Contract Language Example: "*The contractor shall be able to demonstrate the existence of a firewall that is within the Original Equipment Manufacturers (OEM) support lifecycle.*"

2. Can the vendor rapidly assess changes to normal behavior within their network?

   Contract Language Example: "*The contractor shall have technical mechanisms to identify unanticipated changes within their network to include network of host-based Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) to include monitoring of on-premise and cloud based computing assets."*

3. Does the vendor use and require multifactor authentication (MFA)?

   Contract Language Example: "*The contractor shall have a multifactor access control solution in place to limit access to administrative accounts, computing assets with Personally Identifiable Information (PII), Criminal Justice related data and/or system information, or Protected Health Information (PHI)"*

4. Does the vendor have malware protection in place on all endpoints, including servers?

   Contract Language Example: "*The contractor shall have antivirus and malware protection throughout their enterprise, including servers. The company providing the solution shall not include Kaspersky Labs or Trend Micro due to national security concerns identified by the U.S. Federal Government."*

Why this is important

The suggested content above illustrates to the contractor that the expectation for having basic cyber hygiene is codified by contractual language. This will only be as valuable as the local or State agency's provisions for formal sanctions or other punitive actions when a violation occurs.

Alignment: NIST SP-800-53 (AC-2) (SI-3), NIST SP800-171 (3.1.1), CERT-RMM (IR.2.093) (AU.2.044) (SC.2.179) (RM.3.147), NIST SP800-161 (AC-4) & (SA-12:13)

3.2 MEDIA PROTECTION

Media protection is not limited to the realm of cyber. Sensitive information such as tax records, voting records, vehicle registration, criminal records, health information, and citizen payment (credit card data) information may exist in hard copy. An industry best practice is to define levels of information to create categories. Former naming conventions may include "For Official Use Only". The National Archives and Records Administration (NARA) has defined a list of data categories that are now defined as CUI.[10]

While State and local governments are not inherently bound by these new definitions, it is important to note that once any of these data sets are transmitted to or received from the Federal Government, the safeguarding requirements become enforceable.

1. Does the vendor have media protection controls in place?

   Contract Language Example: "*The vendor shall protect (i.e., physically control and securely store) information system media containing sensitive information as defined by our agency, both paper and digital*."

   "*The vendor shall have implemented cryptographic mechanisms to protect the confidentiality of information stored on digital media during transport outside of controlled areas unless otherwise protected by alternative physical safeguards prior to the commencement of the contract."*

   "*The vendor shall prohibit the use of portable storage devices when such devices have no identifiable owner. When sensitive information is to be stored on portable devices, it shall be encrypted."*

[10] NARA CUI Registry, https://www.archives.gov/cui/registry/category-list

"*The vendor shall have cryptographic mechanisms equivalent to AES-256 encryption on assets where sensitive data resides at rest or in transport within the vendor's owned or controlled networking infrastructure (including cloud).*"

"*The vendor shall sanitize or destroy system media containing agency sensitive information before disposal or release for reuse. Proof of sanitization or destruction is required in writing by vendor leadership with signing authority*"

Why this is important

The suggested content would have significantly reduced the likelihood of the harm experienced by State and local agencies in 2019. This content limits the exposure to harm associated with privacy and cybersecurity requirements when best practices are not followed by the vendor.

Alignment: NIST SP-800-53 (MP-1) (MP-2) (MP-5), and NIST SP800-171 (3.8.1) (3.8.6)

3.3 INCIDENT RESPONSE

After human error, Incident Response is statistically one of the single highest areas of failure by enterprises (public and private sector). The NIST CSF has two of the five functions of the framework dedicated to incident response coordination. Even if your supply chain can demonstrate the operational and technical mechanisms described in the access control and media protection sections above, an inability to properly respond to a cyber or privacy event can be very time and cost intensive.

FACTOID: Did you know that between 75%-80% of a cyber insurance policy is exhausted during the incident response phase?[11] This leaves little financial bandwidth to address other critical matters a vendor or contractor may encounter. A lack of having an incident response plan may even preclude the company from obtaining cyber liability insurance.

The ability to demonstrate that the vendor's incident response plan will include the agency points of contact for their external call tree procedures will likely reduce a delay in the containment and eradication phases of an incident response scenario. The level and maturity of such incident response capabilities can even be considered as an evaluation criterion.

1. Does the vendor have an Incident Response Plan (IRP)?

[11] National Association of Insurance Commissioners Spring National Meeting, April 2017

NOTICE: A Disaster Recovery Plan is not the same as an IRP.

Contract Language Example: "*The vendor shall have a preexisting Incident Response Plan that is evaluated annually for applicability."*

"The vendor shall have conducted a table-top exercise of the IRP at least annually."

"The vendor shall track, document, and report incidents to appropriate organizational officials and/or authorities."

2. Does the vendor have an IRP that already established specific points of contact with each State it either conducts commerce in and/or has PII of citizens from within each state?

   "The vendor shall have a preexisting breach notification strategy that conforms with all 50 State laws."

Why this is important

The suggested content will significantly reduce the likelihood of the harm experienced by State and local agencies stemming from dwell time by improving operational effectiveness and efficiency by the vendor.

Alignment: NIST SP-800-53 (IR-2) (IR-3) (IR-4), and NIST SP800-171 (3.6.1) (3.6.3) (3.6.3)

3.4 SOFTWARE ASSURANCE

As the adoption of new Internet of Things (IoT) technologies have evolved, industry best practices to protect the code base from malicious interference have not kept up. As of 2019, the U.S. Departments of Defense and Commerce have banned certain technologies because of intentional code-related issues that allow for unapproved access by the OEM to U.S. Government information systems where the software resides.

The Open Web Application Security Project (OWASP)[12] is widely accepted as the leading guidance for commercial enterprises to adopt best practices to ensure source code is designed in a safe and secure manner. This guidance provides principals that focus on ten core areas commonly associated with creating vulnerabilities in software code.

[12] OWASP Top 10; https://owasp.org/

1. Does the vendor conduct an independent security evaluation of the software? If yes, can the vendor provide proof of such a review?

   Contract Language Example: "*The software being provided has undergone a comprehensive code review and included a static and dynamic source code review with a report of compliance within the last calendar year from date of award.*"

2. Where was the code created and/or produced?

   Contract Language Example: "*The software being provided now or in the future shall not be compiled or processed in any manner within China, Russia, Ukraine, Iran, or North Korea. If the code is deemed mission critical and no other source country can produce, our agency has the exclusive right to review and accept the risk or deny without claims of harm by vendor."*

Why this is important

The suggested content should significantly reduce the likelihood of unforeseen vulnerabilities in software coding practices that result in scenarios allowing for the exploitation of said code and thus allowing for remote command and control of system resources by unauthorized parties.

Alignment: NIST SP-800-53 (MA-3) (SI-3), NIST SP800-171 (3.7.4) (3.14.5), and CERT-RMM (CA.3.162)

3.5 RISK MANAGEMENT

Implementing requirements as they apply to technical and operational safeguarding controls are important; however, not all risk mitigation strategies can be exclusively tied to these controls. More money is spent on cyber and privacy defense technologies today than ever before. The risk postures of enterprises (public and private sector) are not improving proportional to these levels of spending. This section of the document will highlight additional considerations when determining an appropriate vendor or contractor to do business with.

1. Does the vendor have cyber liability insurance? If so, does it include first and third-party damages?

   Contract Language Example: *"The vendor shall provide a copy of their cyber liability policy with an expiration no less than after the base year of performance or demonstration of ongoing coverage for no less than two years to our agency."*

NOTICE: It is the responsibility of each local or State agency to independently determine the exposure value to properly determine adequate levels of insurance coverage ($1M, $5M, etc.).

2. Has the vendor undergone an Independent Verification and Validation (IV&V) assessment within the past year?

   Contract Language Example: *"The vendor shall have undergone and independent assessment of their cyber risk posture. If a Report of Compliance (ROC) exists, it will be made available to the agency at the discretion of government. If the vendor performs internal cyber and privacy risk assessments, it must do so annually and have clearly defined plans of actions and milestones."*

3. Does the vendor have established policies and procedures for Access Control, Media Protection, and Incident Response?
   Contract Language Example: *"The vendor shall have established corporate policies that apply to the safeguarding of system resources (including our agency's) that cover access controls, media protection and incident response."*

4. Does the vendor require annual security and privacy training for its employees?

   Contract Language Example: *"The vendor shall have an annual training program that includes cybersecurity best practices (including phishing training content) and privacy best practices (basis of information collection, storage and transmission)."*

5. Does the vendor accept the right to audit?

   Contract Language Example: *"The vendor implicitly acknowledges and approves the right of our agency to audit all applicable artifacts associated with the vendor's representations and certifications of conformance with our cybersecurity and privacy requirements. Violations may include up to contract termination and false claims acts."*

Why this is important

The suggested content significantly reduces the likelihood of harm to State and local agencies from gaps in operational and managerial practices that lead to technical vulnerabilities.

Alignment: NIST SP-800-53 (CA-2) (CA-5), NIST SP800-171 (3.12.1) (3.12.2), and CERT-RMM (RM.3.144)

APPENDIX A – REFERENCES

1. National Institute of Standards and Technology Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, March 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5-draft.pdf
2. National Institute of Standards and Technology Special Publication 800-171, Revision 1, Protecting Controlled Unclassified Information in Non-Federal Systems and Organizations, February 2020. https://doi.org/10.6028/NIST.SP.800-171r1
3. Open Web Application Security Project Top Ten, 2017. https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/
4. National Archives and Records Administration Controlled Unclassified Information Registry, 2020. https://www.archives.gov/cui/registry/category-list
5. 5 Reasons Why Supply Chain Security Must be on your Radar, Venture Beat Magazine (2020). https://venturebeat.com/2020/01/08/5-reasons-why-supply-chain-security-must-be-on-your-agenda/
6. 8 Cities that have been crippled by cyber-attacks", Business Insider (2020). https://www.businessinsider.com/cyberattacks-on-american-cities-responses-2020-1
7. Overview: 30 Small Business Cyber Security Statistics, Fundera (2020). https://www.fundera.com/resources/small-business-cyber-security-statistics
8. Cyber Liability Study, NetDiligence (2019) https://netdiligence.com/wp-content/uploads/2018/11/2018-NetDiligence-Claims-Study_Version-1.0.pdf

9. Internet of Things Security Acquisition Guidance (2020) https://www.cisa.gov/sites/default/files/publications/20_0204_cisa_sed_internet_of_things_acquisition_guidance_final_508_0.pdf
10. "Threat Evaluation Working Group: Threat Scenarios", U.S. Department of Homeland Security (2020). https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report_0.pdf
11. National Institute of Standards and Technology Special Publication 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations" https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf
12. U.S. Department of Homeland Security , "Trust is Smart Cities System Report" https://www.cisa.gov/sites/default/files/publications/Trust%20in%20Smart%20City%20Systems%20Report_0.pdf