



Supply Chain Security Standard

Introduction

Supply chain security is a critical component of the OMES Information Services information security program. OMES is committed to identifying, evaluating and mitigating potential risks associated with external suppliers, vendors, logistics and transportation for the State of Oklahoma by preventing incidents that may impact confidentiality, integrity or availability of information assets for the state.

The United States federal government maintains a list of equipment and services that pose a threat to national security. The risks posed by these data security threats include but are not limited to unauthorized access to the state network, sensitive state data and individual personal data. OMES prohibits the use or acquisition of services and products from these organizations, or any of these organizations' predecessors, successors, parents, subsidiaries or affiliates, that are named on the Federal Communications Commission's threat list.

State policy also requires the performance of regular third-party cyber management security reviews to identify risk and ensure appropriate controls are in place. TPCM security reviews allow the alignment of information security with business objectives and regulatory requirements.

TPCM and related security reviews take many forms (e.g., security assessments, software reviews, risk analysis platform, configuration analysis and/or vulnerability scanning and testing). They all have the same goal: to improve overall security posture by identifying and acting on current and potential risk.

Identifying information security risk and control requirements from vendor onboarding is essential and far less costly than retrofitting or addressing the impact of a security incident. Furthermore, these security reviews allow management to prioritize and focus on areas that pose the most significant impact on critical and sensitive information assets, providing the foundation for informed decision-making regarding cybersecurity.

As per OMES IS policy, any vendor that is or will be hosting, storing, transmitting, processing and /or accessing State of Oklahoma data or having direct access to State of Oklahoma information systems on premises must be properly assessed and managed for risk and undergo a TPCM security review as part of its business partnership life cycle. Vendors will then be granted Authority to Operate (ATO) with state agencies. No vendor can do business with the state without a valid ATO.

Purpose

This document provides guidance on certain services, products or supplies identified on the national security threat list and establishes the requirement for TPCM security reviews. TPCM security reviews are required for vendors that are, or will be, hosting, accessing, processing, transmitting or storing State of Oklahoma data in compliance with OMES IS security policies, standards and procedures.

Definitions

- ATO – Authority to Operate; an assertion that the supplier's internal security policies meet the minimum standards set by OMES Oklahoma Cyber Command.
- Tier 3: Low criticality – Any system or data intended for public disclosure. The loss of confidentiality, integrity or availability of the system or data would have no adverse impact on safety, finances or reputation.
- Tier 2: Medium criticality – Any system or data not generally available to the public. The loss of confidentiality, integrity or availability of the system or data could have a mildly adverse impact on safety, finances or reputation.
- Tier 1: High criticality – Any system or data protected by law or regulation (e.g., FTI, CJI, PHI, PII and PCI). The loss of confidentiality, integrity or availability of the data or system could significantly and adversely impact safety, finances or reputation. This type of risk requires the state to self-report to the regulatory entity and/or notify the individual if data is inappropriately accessed.
- Vendor – Any supplier, contractor, service provider, consultant or any other individual and/or organization external to state government providing services on behalf of, for, or as an agent of state government.

Standard

OMES prohibits the use or acquisition of any services or products from suppliers or subsidiaries:

- on the FCC national security threat list;
- located in, or have close ties to, a country or regime that has current sanctions levied against them by the U.S. or their allies.

The state agency shall categorize data as confidential by system owners, including protected health information and personally identifiable information, in accordance with applicable federal and state laws, directives, standards, guidance, policies and regulations.

OMES IS shall conduct third-party cybersecurity reviews. The review will address the likelihood and magnitude of harm should there be unauthorized access, use, disclosure, disruption, modification or destruction of the information system and the information it processes, stores or transmits. Additionally, these guidelines apply to risk assessments:

- OMES IS will document the results of the annual security review.
- OMES IS will review risk analysis results annually.
- OMES IS will disseminate security review results to stakeholders.
- OMES IS will update the third-party security review annually or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities) or other conditions that may impact the system's security state.

All vendors given access to State of Oklahoma information, information systems or information assets must complete a security review. The purpose of the review is for the State of Oklahoma to identify and manage the risk stemming from the business partnership.

A vendor is required to complete a TPCM security review if hosting, accessing, processing, storing or transmitting State of Oklahoma data. The review is not restricted to a specific service or solution but is for the vendor to be assessed from an internal security standpoint (organizational policies, standards, procedures, guidelines and controls). The security of hardware, software, IT solutions and/or IT services being acquired should have no bearing on the enterprise security controls of the vendor.

Industry-standard assessments and certifications may be used in lieu of the OMES IS review if they are substantially similar in structure and content. The following industry-standard assessments and certifications are approved:

- SIG Lite for Tier 2 and 3 vendors.
- SIG Core for Tier 1, 2 and 3 vendors.
- CSA CAIQ v3.1 for Tier 1, 2 and 3 cloud service providers.
- CSA CCM/CAIQ v4 for Tier 1, 2 and 3 cloud service providers.
- FedRAMP for Tier 1, 2 and 3 cloud service providers.
- StateRAMP for Tier 1, 2 and 3 vendors (preferred for cloud service providers).
- ISO 27001 for Tier 2 and 3 vendors.
- HITRUST for Tier 1, 2, and 3 vendors.
- AICPA SOC 2 Type II for Tier 1, 2, and 3 vendors (Must cover all 5 Trust Services Criteria).
- DoD CMMC 2.0 Level 2 or 3 for Tier 2 and 3 vendors.

Compliance

This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale

To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

References

- [List of Equipment and Services Covered by Section 2 of The Secure Networks Act.](#)
- [U.S. Department of State Economic Sanctions.](#)
- National Institute of Standards and Technology Special Publications: NIST SP 800- 53a –Risk Assessment, NIST SP 800-12, NIST SP 800-30, NIST SP 800-39, NIST SP 800-40, NISTSP 800-70, NIST SP 800-100 and NIST SP 800-115; NIST Federal Information Processing Standards 199.
- [Third-Party Cyber Management.](#)
- [Attachment D State of Oklahoma IT Terms.](#)
- [State of Oklahoma Information Security Policy, Procedures, Guidelines.](#)
- [Cloud Security Alliance \(CSA\).](#)
- [Shared Assessments \(SIG\).](#)
- [FedRAMP Authorization Management Program.](#)
- [StateRAMP.](#)
- [International Organization of Standardization \(ISO\).](#)
- [DOD CMMC 2.0.](#)

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 06/11/2025	Review cycle: Annual
Last revised: 06/17/2025	Last reviewed: 06/17/2025
Approved by: Dan Cronin, Chief Information Officer	