U.S. General Services Administration

Draft Guidance on Software Licensing Management

April 24, 2026

Office of Government-wide Policy
Technology Transformation Services

Table of Contents

Executive Summary

The General Services Administration (GSA) is submitting this draft guidance document to fulfill a requirement in the joint explanatory statement accompanying the Consolidated Appropriations Act, 2026 (Public Law 119-75). This joint explanatory statement directs GSA's Office of Government-wide Policy and Technology Transformation Services to report to the Committee with a draft version of joint guidance for implementing fair software licensing principles and technology license tracking in Federal agencies. GSA intends to publish a final guidance document by September 30, 2026, on GSA.gov.

This draft guidance is built on existing statutory and policy requirements related to software license management, acquisition, and security, including the Federal IT Acquisition Reform Act (FITARA) of 2014, the MEGABYTE Act of 2016, and Executive Order 14028, and "Improving the Nation's Cybersecurity." Despite this legislative framework, multiple Government Accountability Office (GAO) reports indicate that agencies continue to struggle with maintaining accurate software license inventories and optimizing license usage.

To address this persistent gap, this draft guidance establishes recommended principles for fair software licensing and a minimum baseline for technology license tracking. Effective software license management enables federal agencies to optimize software usage, achieve significant cost savings and avoidance, mitigate cybersecurity risks, and ensure compliance.

To maximize the effectiveness of this draft guidance, agencies should prioritize the following explicit, high-level activities. These steps set the context for the detailed narrative that follows and are the minimum requirements for achieving effective software license management.

Recommended Agency Activities for Software License Management

- **Establish Governance:** Agencies should establish minimum governance roles. All software acquisitions, renewals, usage, and retirements should be managed through a documented, cross-functional internal control and governance structure rather than through isolated, program-level transactions.
- **Maintain Comprehensive Inventory:** Agencies should maintain a comprehensive software license inventory that captures enough information to support asset management, compliance, budgeting, security, and procurement decisions.
- **Implement Technology Solutions:** Agencies are recommended to leverage a suite of interoperable technology solutions, such as software asset management tools and software-as-a-service (SaaS) management platforms, allowing the tracking of license usage, the monitoring of expiration, and the optimizing of utilization.

- **Conduct Regular Audits:** To ensure licenses are in compliance, agencies should integrate recurring reviews and audits as a regular governance task for periodically reconciling software usage against purchases to verify usage rights, detect licensing gaps, and inform renewal decisions.
- **Proactively Manage License Renewal:** To prevent costly automatic renewals and ensure mission continuity, agencies should establish a mandatory review period (at least 3 months prior to expiration) to assess license utilization, compliance, and cost-saving opportunities, and receive advance notification of renewal terms.
- **Follow Recommended Principles:** Agencies should adhere to the 10 recommended Fair Software Licensing Principles to promote transparent, reasonable, and non-discriminatory licensing terms.
    1. **Bona Fide Need:** Agencies should ensure software is procured and assigned to support a genuine mission need, funded by appropriations from the fiscal year in which the software is actually used.
    2. **Price and Term Transparency:** Seek terms that are clear, non-discriminatory, and easily understandable to determine all licensing costs, including the up-front disclosure of any hidden fees. Terms should also allow for sharing of prices and discounts across the Federal Government.
    3. **Total Cost of Ownership (TCO):** Agencies should evaluate TCO, which includes all associated expenses like maintenance, migration, support, training, and exit costs, rather than focusing solely on the seat price.
    4. **Clear Entitlement and Metric Definitions:** Licenses should precisely define the purchase entitlement, its measurement metric (e.g., user, core), and the organizational scope to which it applies. In addition, agencies should retain the right to reassign unused or inactive licenses across the enterprise.
    5. **Vendor Accountability:** Agreements should include clear service level agreements (SLAs), defined support obligations, and performance guarantees with specified remedies for non-compliance. In addition, vendors should commit to regular security updates and timely patch deployments.
    6. **Trackability by Design:** Agencies should prefer software products and terms that allow continuous monitoring and tracking using software asset management tools across the entire license life cycle. This continuous monitoring supports optimization, reconciliation, and compliance efforts.
    7. **Reasonable Audit Practices:** Audit clauses should include reasonable notice, a clear scope, confidentiality protections, the use of existing records, and proportionate remediation to foster effective relationships with vendors.
    8. **License Life cycle Management Pre-renewal and Orderly Transitions:** Licenses should include an advance renewal notice to ensure agencies conduct a pre-renewal review (at least 3 months prior) to assess utilization and optimization opportunities. License purchase agreements should also include documented data export rights to mitigate vendor lock-in risk.
    9. **Accessibility, Security, and Privacy Compliance:** Agencies should ensure all software licensing and contracting terms fully comply with federal

requirements for accessibility, privacy, and security, including adherence to federal security frameworks for cloud services.

10. **Government-wide Comparability:** Agencies should use common definitions and data fields to allow comparison of prices, usage, and risks across all agreements. This includes standardizing SaaS billing data using the FOCUS specification and adopting the manufacturer part number (MPN) for product identification.

Introduction: Policy and Regulatory Framework

Federal policy on software license management has evolved over time, beginning with A-130, Managing Information as a Strategic Resource. As the foundational policy for federal resource management, A-130 requires agencies to regularly inventory physical and software assets.[1] Since then, many key laws and policies have been enacted to improve license management practices, such as:

- **Federal IT Acquisition Reform Act (FITARA) of 2014:** This Act assigns explicit responsibilities to Chief Information Officers (CIOs), including oversight for IT purchases, approval of major IT contracts and acquisitions, and risk categorization and performance evaluations of vendors. CIOs are also required to optimize their agency's IT portfolio over time.
- **Federal Information Security Modernization Act (FISMA) of 2002 (updated 2014):** Empowers the Department of Homeland Security (DHS) to administer and oversee information security policies for federal executive branch civilian agencies.[2] The Act's relevance to license management is significant, as failure to inventory or properly manage software licenses may unintentionally expand an agency's cyber attack surface.
- **Make Electronic Government Accountable by Yielding Tangible Efficiencies (MEGABYTE) Act of 2016:** Congress passed this Act requiring CIOs to establish and maintain a comprehensive software license inventory and report annually to the Office of Management and Budget (OMB) on financial savings and cost avoidance achieved through improved management.[3]
- **Executive Order (EO) 13103 (September 1998)**: This was one of the earliest policies instructing agencies to account for all installed software,[4] primarily to prevent the government from unintentionally enabling or participating in computer software piracy.[5]
- **Executive Order (EO) 14028, "Improving the Nation's Cybersecurity" (May 2021):** This EO significantly impacts software life cycle management by mandating standards for the security of the federal software supply chain. Its requirements, such as establishing a software bill of materials (SBOM) for critical software, directly support the MEGABYTE Act's call for comprehensive inventory and provide essential data for risk assessment and compliance.[6]
- **OMB Circular A-11:** This circular governs the preparation, submission, and execution of the federal budget, establishing the framework for IT Capital Planning and Investment Control (CPIC). Its requirements for rigorous justification and

[1] https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf
[2] https://www.cisa.gov/topics/cyber-threats-and-advisories/fisma
[3] https://www.congress.gov/bill/114th-congress/house-bill/4904/text
[4] Software licenses subscriptions can be perpetual, subscription based, term, concurrent, enterprise, or open. See Appendix A.
[5] https://www.govinfo.gov/content/pkg/WCPD-1998-10-05/pdf/WCPD-1998-10-05-Pg1941.pdf
[6] https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf

performance monitoring of major IT acquisitions ensure that large software license agreements are evaluated against TCO, providing the essential financial and life cycle data needed for license optimization.[7]

- **OMB Memorandum M-16-12 (2016):** This guidance aims to improve the acquisition and management of software licensing.[8] It encourages agencies to use centralized and collaborative software management platforms[9] for license usage tracking and conduct thorough market research on software license pricing to ensure that agency commercial license agreements are consistent with customary practices, and effectively meet agency needs.[10]
- **OMB Memorandum M-26-05[11] (Rescission and Encouragement):** This memorandum encourages agencies to "continue to maintain a complete inventory of software and hardware" and develop assurance policies that align with their risk determinations and mission needs, without mandating specific security attestations from vendors.[12]

Software license acquisition is also governed by the bona fide needs rule, which requires agencies to obligate fiscal year appropriations only for legitimate needs arising in that same year. Need must be established at contract award, task order placement, or option year, meaning agencies may only acquire licenses they genuinely need and must pay for them with funds from the fiscal year in which they are used, unless multiyear or other authority applies.

Taken together, this legislative and policy framework established a clear statutory baseline for federal software license management. Despite these efforts, multiple reports from GAO found that agencies continue to face challenges in maintaining accurate software license inventories and effectively managing and optimizing their license usage over time.[13] [14] [15] This persistent gap underscores the necessity for the detailed guidance on fair software licensing principles and technology license tracking that follows.[16]

[7] https://www.whitehouse.gov/wp-content/uploads/2025/08/a11.pdf
[8] https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m-16-12_1.pdf
[9] For example, asset discovery and business intelligence (BI) tools.
[10] https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m-16-12_1.pdf
[11] Obtaining security attestations from IT vendors prior to license purchases was initially mandated in 2022 and 2023, and subsequently rescinded by OMB M-26-05.
[12] https://www.whitehouse.gov/wp-content/uploads/2026/01/M-26-05
[13] https://www.gao.gov/products/gao-24-105717
[14] https://www.gao.gov/products/gao-24-106137
[15] https://www.gao.gov/products/gao-25-107114
[16] https://www.gao.gov/products/gao-24-105717

With the proliferation of license types,[17] software license management[18] is key. Software license management is an overarching term that includes managing both software licenses and SaaS subscriptions to cloud-hosted services. Federal agencies have been encouraged by GAO to "create formal policies or guidance that require teams to analyze, track, and mitigate licensing restrictions during IT acquisitions."[19] NIST SP 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations incorporated specific configuration management controls guiding agencies to track software assets and comply with software usage restrictions.[20]

Software management enables federal agencies the ability to optimize their software usage, realize significant cost savings and cost avoidance, mitigate cybersecurity risks, and ensure compliance avoiding license/contract penalties.[21] Effective software license management generally consists of:

1. Comprehensive Software License Inventory
2. Regular Audits

Comprehensive Software License Inventory

Technology license tracking is the set of agency data, processes, and controls used to identify:

- what technology rights the agency acquired,
- where and by whom they are used,
- what they cost,
- what restrictions apply,
- when they renew or expire,
- the relevant maintenance requirements and processes,
- whether use is compliant with terms, and
- where optimization, consolidation, or transition action is needed.

To effectively track licenses, agencies should maintain a **comprehensive software license inventory** that captures enough information to support asset management, compliance, budgeting, security, and procurement decisions.[22] This inventory should explicitly include all

[17] See Appendix A.
[18] Software license management involves tracking and controlling use of software licenses, including but not limited to inventory of licenses, usage monitoring, and ensuring compliance with terms and conditions set by the vendor.
[19] GAO-25-107114, Cloud Computing: Agencies Need Guidance to Address the Effects of Restrictive Software Licenses. https://www.gao.gov/products/gao-25-107114GAO-25-107114, Cloud Computing: Agencies Need Guidance to Address the Effects of Restrictive Software Licenses. https://www.gao.gov/products/gao-25-107114
[20] NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations: Secuirty controls CM-8 and CM-10: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
[21] See Appendix C for more information on cost savings and cost avoidance metrics.
[22] Per GAO, the Biannual Scorecards Report, "in December 2020, all 24 agencies had comprehensive inventories and analyzed software usage to make cost-effective decisions. As a result, the software licensing component

software assets, **including Open Source Software (OSS)**, regardless of acquisition method (procured or freely acquired) or financial cost, to prevent unmonitored use and ensure continuous risk assessment of all deployed assets. Agencies should align this with software asset management, IT asset management (ITAM), and federal guidance such as FITARA and M-16-12. An agency's license inventory and tracking processes should include the following:

1. A complete list of the software license agreements the agency has entered into.[23]
2. A centralized, comprehensive inventory of every license used within the agency that reflects changes in near real-time.
3. Recurring reviews or audits of the licenses, including recommendations on whether they should be reassigned or discontinued. These reviews should be conducted at a cadence that meets the agency's budget needs, such as quarterly, semiannually, annually.

Table 1 summarizes the information that should be included in the agency's comprehensive software license inventory. Appendix D lists a set of core, recommended, and optional data fields that should be included for each category.

Table 1: Recommended Information for Software License Inventory

Category	Definition
License and Entitlement[24] [25]	Details about the license rights and structure, including but not limited to license type, license model, license start date, renewal date, term and expiration. This should include the specific quantities of each license level included in the agreement (e.g., administrator, standard).
Software Identification[26] [27]	Basic information about the software product, including but not limited to software title/product name, software publisher/vendor, versions/editions included in the agreement, and software category.
Procurement & Contract[28]	Links to license acquisition records, including but not limited to vendor name, contract vehicle, contract number, reseller, purchase date, and purchase cost.

was removed from the scorecard. While the removal of this component is evidence of improvement, agencies' continued efforts over managing software licenses remains important."
https://www.gao.gov/assets/gao-22-105659.pdf

[23] This complete list should include any open-source software the agency uses. See Appendix A for more information on open-source and other software license types.

[24] Agencies should use standardized names for the license types and levels to avoid misreporting or duplication.

[25] Agencies need to compare license inventories with purchase records to identify cost savings and ensure compliance. https://www.gao.gov/products/gao-24-105717

[26] Agencies should use standardized naming for the vendors and software versions to avoid misreporting or duplication.

[27] GAO emphasizes establishing comprehensive inventories to ensure agencies can track licenses and compare usage vs. purchases. https://www.gao.gov/products/gao-24-105717

[28] A GAO report recommends detailed inventories including contract terms to enable cost and compliance analysis. https://files.gao.gov/reports/GAO-25-108475/index.html

Category	Definition
Deployment & Usage[29]	Track where and how the software is being used, including but not limited to number of users/devices assigned, number of installations, number of active users,[30] license consumption count, and short descriptions of all use cases the software is being used for. This should also include a list of the specific user/device each license is assigned to.
Infrastructure[31]	Information about the environment supporting the software, including but not limited to the host server or environment, operating system, cloud provider and virtualization environment.
Compliance & Risk[32]	Information about license allocation and utilization levels, including license utilization percentage, audit history, and compliance status (e.g., compliant, over-utilized, under-utilized).
Security & Governance[33]	Relevant security information about the software, including end-of-lifedate, end-of-support date, relevant authorization to operate (ATO) renewal date(s), patching requirements, and FedRAMP authorization status (if applicable).
Ownership & Accountability[34]	List of responsible stakeholders, including but not limited to software owner (business owner), technical owner/system owner, contracting officer, and software asset management Administrator.
Financial and Life cycle Data[35]	Tracks the life cycle and financial impact, such as total cost of ownership, setup cost, operational cost, and maintenance cost.
Documentation[36]	Links supporting documentation, including but not limited to license agreements, vendor terms and conditions and maintenance agreements.

Agencies can adapt the specific structure of their inventory and data collection processes based on their organizational structure. Wherever possible, agencies should prioritize centralization of software license management at the highest agency level to align with the requirements of FITARA and M-16-12.

---

[29] GAO reports that incomplete usage data undermines understanding of whether agencies have the right number of licenses. https://www.gao.gov/products/gao-24-105717

[30] Agencies should define what is considered an "active user" based on a specific time horizon (e.g., 30 days, 90 days) that makes sense for the use case.

[31] https://www.gao.gov/products/gao-14-413

[32] GAO notes agency license inventories should support analysis of use vs. purchase to inform cost decisions and compliance. https://www.gao.gov/products/gao-24-105717

[33] https://files.gao.gov/reports/GAO-25-108475/index.html

[34] GAO recommends centralized governance and oversight to improve software license management consistency.

[35] GAO highlights the need for comprehensive tracking of licenses, including life cycle details, to ensure effective management.

[36] GAO emphasizes sufficient documentation and inventory practices so agencies can demonstrate compliance and avoid redundant licenses. https://www.gao.gov/products/gao-14-413

Regular Audits

Once a comprehensive inventory has been established, the next step is to ensure licenses are in compliance. Regularly reconciling software usage against purchases is a core component of license auditing.[37] This involves establishing a solid structure to verify usage rights, detect over- and under-licensing, validate security and compliance status, and support renewal decisions. The following data points should be gathered during a license audit:

- **License gap analysis**: How many licenses are used compared to how many are purchased (e.g., overuse, underuse). Audits should account for licenses not used due to personnel turnover.
- **True-up/true-down quantity:** The quantified adjustment required to reconcile discrepancies between licensed entitlements and actual consumption, typically used for contract settlement or renewal.
- **Last audit date**: Time of most recent audit.
- **Security authorization status**: Whether the software has an active authorization to operate (ATO).[38]

Technology Solutions

Federal agencies typically address **software license inventory tracking, audits, and compliance** through consistent processes and technology solutions to align with federal requirements like FITARA, MEGABYTE Act, and OMB guidance. Using a software asset management tool is recommended as this allows tracking of license usage, monitoring expiration, optimizing utilization, and managing contracts. Since no single tool performs all the necessary functions for comprehensive auditing, federal agencies can deploy a suite of interoperable technology solutions to meet their auditing needs. Using these interoperable solutions enables agencies to track licenses throughout the software life cycle rather than relying on static data from specific points in time.[39] Table 2 below provides examples of the types of tools that can help streamline agency license audits.

[37] https://www.gao.gov/products/gao-24-105717

[38] Agency CIOs are always responsible for issuing ATOs within the agency. In some cases, the ATO process will include reviewing and referencing a FedRAMP authorization package.

[39] The software life cycle encompasses three primary phases: the initial assignment of licenses and subscriptions to employees and systems; the management of licenses and subscriptions during operational use; and the final recovery or reallocation of licenses.

Table 2: Technology Capabilities Needed for License Tracking and Auditing

Tool	Capabilities
Software Asset Management Managed Services[40]	• Automated discovery of installed software across endpoints, servers, and cloud • License entitlement vs. usage reconciliation • Audit trails and compliance reporting • Cost optimization and license re-harvesting
IT Asset Management (ITAM) and Configuration Management Database (CMDB) Platforms[41]	• Centralized asset inventory (devices, software, SaaS) • CMDB • Life cycle tracking (procure → deploy → retire) • Integration with procurement and finance systems
Cyber Asset Attack Surface Management/Visibility Platforms[42] [43]	• Aggregates data from hundreds of systems (network, cloud, SaaS, endpoints) • Identifies unknown/unauthorized software • Continuous monitoring vs. point-in-time inventory • Policy enforcement and compliance validation
Vulnerability & Compliance Scanning Tools[44]	• Verifies • Installed software vs. approved baselines • Unauthorized software • Identify security patching and updates needed
SaaS Management Platforms[45]	• SaaS discovery (often shadow IT) • Subscription tracking and renewal alerts • Cost allocation and optimization

Emerging commercial technologies are available to streamline management of software license inventories and audits. Agencies should evaluate these technologies against their

[40] Software asset management platforms are the core system of record for license inventory, usage tracking, reconciliation, and audit readiness.
[41] These extend software asset management into full life cycle asset tracking, including hardware, software, and cloud services.
[42] Technology Solution focuses on continuous discovery and validation of all assets, providing a unified, real-time view to identify, normalize, and remediate vulnerabilities and misconconfigurations.
[43] For example, the Cybersecurity and Infrastructure Security Agency (CISA) administers the CDM program, which helps agencies continuously monitor software deployed within their environment(s). More information on this program can be found in Appendix E.
[44] These tools are critical for audit evidence and compliance validations; however, they typically do not manage licenses directly.
[45] Manages subscription licenses and usage-based spend in the cloud.

specific needs and governing regulatory policies. To ensure appropriate use, agencies should understand and govern these solutions, maintaining a human in the loop.

Fair Software Licensing Principles

Fair software licensing principles are guidelines that promote transparent, reasonable, and non-discriminatory software licensing terms that allow government customers to deploy, migrate, and use software across different environments (including cloud platforms) with license portability and eliminating excessive costs. The foundational policy framework for implementing these fair software licensing principles is already well established.

To ensure effective technology license tracking across federal agencies, it is necessary to establish minimum governance roles. This structure distinguishes between statutory duties, OMB policy requirements, and recommended practices designed to improve consistency, auditability, and enterprise buying discipline.

All software acquisitions, renewals, usage, and retirements should be managed through a documented, cross-functional internal control and governance structure rather than through isolated, program-level transactions. Appendix B details the roles and responsibilities of the CIO, the Chief Acquisition Officer (CAO), the Chief Financial Officer (CFO), the Software Manager/Team, the General Counsel and Acquisition Counsel, and the Security, Privacy, Records, and Accessibility Leads.

The following principles are recommended as preferred federal practice, inferred from existing authority, policy, oversight findings and best practices:

1. **Bona Fide Need:** Agencies should ensure software is procured and assigned to support agency mission, duties, and obligations, funded by appropriations from the fiscal year corresponding to the software usage.

2. **Price and Term Transparency:** Agencies should seek terms that are non-discriminatory, clear, and unambiguous to readily determine licensing costs—including the up-front disclosure of hidden fees —and allow sharing of prices, discounts, and material conditions across the Federal Government, consistent with M-16-12.[46]

3. **Total Cost of Ownership (TCO):** Agencies should evaluate TCO, including software maintenance, migration, support, training, and exit cost, not just seat price. See Appendix C for cost savings and cost avoidance metrics. **Flexible Consumption and Pricing Models:** Agencies should seek agreements that:

[46] Specifically, M-16-12 explains that "agencies should not agree to terms and conditions that prohibit the sharing of all prices, terms, and conditions for commercial and COTS software licenses with other Government entities." https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-12_1.pdf

a. Permit flexible consumption, allow for the unbundling of products, and ensure the government can realize the best-value pricing and discounts across its total purchase portfolio rather than being restricted to rigid, mandatory product bundles.
b. Provide the ability to scale licenses up or down based on actual usage.
c. Avoid restrictive license terms that could negatively affect costs, cloud migration, and system architecture.[47] Agencies should identify potentially restrictive terms, such as vendor lock-in[48] or conversion fees, during the pre-award portion of the acquisition life cycle (e.g., market research, proposal, evaluation).

4. **Clear Entitlement and Metric Definitions:** Licenses should precisely define the purchase entitlement[49] and its corresponding measurement metric (e.g., user, core, consumption unit).[50]
    a. **Reallocation and Reuse Rights:** Agencies should have the ability to reassign unused or inactive licenses within the agency enterprise, and where feasible, across enterprise scope.
    b. **Defined Enterprise Scope:** Agreements should expressly state the organizational level (e.g., office, bureau, component, agency-wide) to which the software license(s) apply, with license(s) assigned to the highest agency level (e.g., cabinet level) when feasible to maximize portability and usability.

5. **Vendor Accountability:** Agencies should ensure that agreements include the following provisions:
    a. Clear SLAs - Agencies should use standard SLA templates and contract language to establish **clear, consistent, and enforceable expectations** across cloud and software providers.[51,52]
    b. Defined vendor support obligations and response times.
    c. Performance guarantees with specified remedies for non-compliance. Licensing and service agreements should define **how issues will be corrected if the vendor fails to meet service requirements**, including corrective actions or penalties.[53]
    d. Commitments for regular security updates and timely patch deployments.

---

[47] For example, software licenses should allow agencies to move workloads between on-premise systems and cloud environments without paying duplicate licensing costs. See GAO-25-107114, Cloud Computing: Agencies Need Guidance to Address the Effects of Restrictive Software Licenses. https://www.gao.gov/products/gao-25-107114

[48] For example, an AI platform that can only run on Amazon Web Services (AWS).

[49] A purchase entitlement is the documented right or authorization to access, use, or receive a specific product, service, or asset, often based on a purchase order or subscription agreement. It defines the allowed quantity, duration, and scope of what was purchased (e.g., software licenses, 300 phone minutes).

[50] https://fairsoftwarelicensing.com/our-principles/

[51] GAO-24-106137, Cloud Smart: Agencies Need Guidance and Performance Measures to Meet OMB Requirements. https://www.gao.gov/products/gao-24-106137

[52] SLAs specifically apply to cloud-hosted services.

[53] GAO-24-106137, Cloud Smart: Agencies Need Guidance and Performance Measures to Meet OMB Requirements. https://www.gao.gov/products/gao-24-106137

6. **Trackability by Design:** Agencies should prefer terms and products that can be tracked and continuously monitored, using **software asset management tools,** across purchase, deployment, usage, renewal, and retirement to support optimization and license reconciliation.[54] This comparison helps agencies maintain an accurate inventory and ensure compliance of IT assets and configurations.[55] [56]

7. **Reasonable Audit Practices:** Agencies should prefer audit clauses with reasonable notice, clear scope, use of existing records, confidentiality protections, and proportionate remediation. Reasonable audit practices help to establish clear and binding contractual safeguards that foster effective relationships with vendors.

8. **License Life cycle Management: Pre-Renewal Review and Orderly Transition:** Agencies should ensure the following:
    a. Licenses should have an advance renewal notice; agencies should ensure that at least 3 months prior to annual renewal, there is a review of license utilization, compliance, and optimization opportunities.
    b. Contracts for licenses should have documented data export rights that allow for data portability that mitigate vendor lock-in risks.

9. **Accessibility, Security, and Privacy Compliance:** Agencies should ensure the licensing and contracting terms support compliance with Section 508, OMB Circular A-130, and federal laws and regulations, including federal security frameworks (e.g., FedRAMP).[57]

10. **Government-wide Comparability:** Agencies should use common definitions, data fields, and review criteria to compare prices, usage, and risks across agreements. To ensure consistency and support accurate market research and price comparison, this principle includes:
    a. **Data Standardization for Software-as-a-Service (SaaS) and Consumption:** Promote the use of the FinOps Open Cost and Usage Specification (FOCUS), an industry-supported standard, to define requirements for technology billing data. By standardizing cost and usage datasets, agencies can transparently identify, track, and compare software license costs that are frequently bundled within broader cloud service fees. The immediate accessibility of FOCUS data from cloud service providers enables, with supporting services, precise software license reconciliation, accelerates government-wide cost

[54] This principle is essential to helping agencies comply with M-16-12, which requires them to use automated tracking mechanisms for IT asset discovery, inventory tracking, inventory normalization, and license optimization. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-12_1.pdf
[55] This is a direct focus of OMB M-16-12: https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-12_1.pdf
[56] GAO-24-105717, Agencies Need to Better Assess and Achieve Additional Savings from Software License Purchases. https://www.gao.gov/products/gao-24-105717
[57] GAO-24-106137, Cloud Smart: Agencies Need Guidance and Performance Measures to Meet OMB Requirements. https://www.gao.gov/products/gao-24-106137

optimization, and ensures software "consumption" is measurable across all vendor environments.[58]

b. **Standardized Manufacturer Product Identification (MPN):** Use the government-wide use of the MPN from the original equipment manufacturer, rather than reseller-specific SKUs, for all product identification. MPNs should be consistent across the Federal Government and, where applicable, aligned with the commercial marketplace. Using a universal identifier ensures that a specific software license version can be tracked from purchase through its entire life cycle, regardless of the acquisition vehicle used.

[58] https://focus.finops.org/what-is-focus/

Appendix A: Subscription Types for Software Licenses

License Type	Description	Key Implications
Perpetual	Permanent, indefinite rights to use the software after a single, one-time purchase. May require an additional annual fee for maintenance, support, and updates.	Classified as a capital expense (CapEx) requiring higher initial outlay; offers long-term control and predictable costs post-purchase, but carries the risk of technological obsolescence and increased future upgrade costs.
Subscription	Grants the right to use the service for a fixed, limited duration (e.g., monthly, annually). This model is highly common with Software-as-a-Service (SaaS) and cloud-based offerings.	Treated as an operating expense (OpEx) with lower upfront costs and predictable recurring payments; provides flexibility, scalability and automatic updates, but poses a risk of total cost escalation over many years. With each renewal, agencies still need to comply with the bona fide need rule and ensure Section 508 compliance.
Term	Grants time-limited rights to use the software (e.g., 1 year). May require an additional annual fee for maintenance, support, and updates.	A project-friendly OpEx model suitable for short-term initiatives or defined contract periods; offers cost predictability for the licensed duration but requires careful management upon expiration or renewal.
Concurrent	Licensing is based on the maximum number of users or devices that can access and use the software simultaneously, regardless of the total number of installed copies. Can be either perpetual or term in duration.	Maximizes software utilization for agencies with shared resources or shift workers; requires robust usage tracking and compliance monitoring to avoid penalties for over-utilization.
Enterprise/Site	A blanket license that permits unlimited use across an entire agency, department, specific physical location, or by a defined population of users (e.g., all federal employees).	Greatly simplifies license management and compliance and typically enables the highest volume discounts; however, it risks substantial "shelfware" (unused licenses) if adoption is not widespread (over-licensing).
Open Source	Primarily managed by a combination of parties, including non-profit foundations, corporations, and the public, who	Benefits include significant cost savings and unparalleled flexibility and customization. However, it requires a thorough understanding and strict

License Type	Description	Key Implications
	grant rights to freely use, modify, and distribute the software's source code, often at no financial cost, under specific terms (e.g., GPL, MIT licenses).	compliance with the specific license terms and mandates the agency to secure its own technical support arrangements. Risks include the software being unmaintained, orphaned, discontinued, or vulnerable to security risks due to modification by external parties.

Appendix B: Roles and Responsibilities

Role/Function	Key Responsibilities and Actions
Chief Information Officer (CIO)	Oversee IT planning, budgeting, governance, acquisition approval, and software life cycle management. Sets agencywide software policy, approves IT budget, and reviews and approves IT contracts (with limited delegation exceptions). Routes new software acquisitions, renewals, and exceptions through a governed approval chain.[59] [60] [61]
Chief Acquisition Officer (CAO) and Procurement Function	Translates enterprise policy into acquisition discipline. Ensures acquisition strategies, plans, and interagency agreements involving IT have CIO review/approval. Owns contract strategy, vehicle selection, renewal controls, market research, and negotiation. Conducts a review before renewing or exercising an option to determine whether the renewal or option is "in the government's best interest."[62] [63] [64]
Chief Financial Officer (CFO) and Finance Function	Provides financial transparency. Works with CIO to ensure that budgeting and reporting reflect the full scope of software obligations, subscriptions, maintenance, and associated funding. Maintains unit-cost views and common savings methodologies. Reviews enterprise software business cases and aligns invoices to the license inventory.[65] [66]

[59] https://www.congress.gov/bill/113th-congress/house-bill/1232
[60] https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf
[61] https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf
[62] https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf
[63] https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m-16-12_1.pdf
[64] https://www.acquisition.gov/far-overhaul/far-part-deviation-guide/far-overhaul-part-17#FAR_17_204_1
[65] https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf
[66] https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m-16-12_1.pdf

Role/Function	Key Responsibilities and Actions
Software Manager/Team	The operational center for license tracking, consumption management, and continuous optimization (reports to the CIO). Maintains a continual agencywide inventory of licenses (including SaaS). Automates asset discovery and reconciliation. Analyzes usage data to identify duplication, underutilization, and compliance risks. Develops the agency's software management centralization approach. Generates reports and dashboards for enterprise review.[67]
FinOps Team	Serves as the enterprisewide financial accountability and governance function, reporting directly to the CIO, CFO, and CAO to ensure unified oversight of technology spending, driving fiscal responsibility for software consumption and cloud services. Primary responsibility is establishing and maintaining financial transparency by aligning consumption data with budget practices, driving continuous optimization to realize cost savings and cost avoidance.
General Counsel and Acquisition Counsel	Reviews software license terms as a material governance control, especially nonstandard terms. Reviews nonstandard End-User License Agreements, audit clauses, data-rights terms, and other dispute-sensitive provisions. Issues a documented legal sufficiency review for significant deviations.[68] [69] [70]
Security, Privacy, Records, and Accessibility Leads	Validate vendor compliance with federal requirements throughout the software acquisition life cycle. Incorporate security and privacy requirements into contracts. Ensure records management and retention are incorporated throughout the information life cycle. Validate compliance before award, at renewal, and upon material change.[71] [72] [73]
Program/Business Owners and Component CIOs	Provide input on the mission needs that need to be addressed through enterprise software solutions, verify adoption and usage of the solutions before renewals or quantity increases, and document and share evidence needed to make governance decisions, such as business cases, usage attestations, and transition plans.[74] [75] [76]

[67] https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m-16-12_1.pdf
[68] https://www.acquisition.gov/far/27.405-3
[69] https://www.acquisition.gov/far/52.227-19
[70] https://www.archives.gov/records-mgmt/policy/records-mgmt-language
[71] https://www.section508.gov/manage/laws-and-policies/
[72] https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf
[73] https://www.whitehouse.gov/wp-content/uploads/2026/01/M-26-05
[74] https://www.congress.gov/bill/113th-congress/house-bill/1232
[75] https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m-16-12_1.pdf
[76] https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf

Taken together, these roles establish a control system in which software demand, legal terms, security and records compliance, funding, and inventory data converge before an agency acquires, renews, expands, or retires software. Agencies should document the workflow and decision artifacts for each trigger event—including new awards, option exercises, true-ups, SaaS migrations, major modifications, and exception requests—so that fair licensing and reliable technology license tracking become repeatable enterprise practices rather than one-time procurement exercises.

Appendix C: Cost Savings & Cost Avoidance Metrics

A. Cost Savings Metrics[77] [78]

Measures realized reductions in software spending through proactive management.

Table 3: Example of Cost Saving Metrics

Metric	Definition	Calculation/Data Source[79]
License Reclamation Savings	Savings from reclaiming unused or underutilized licenses	Number of reclaimed licenses multiplied by cost per license
SaaS Subscription Optimization Savings	Savings realized from identifying and terminating unnecessary or underutilized SaaS subscriptions, user accounts, or module entitlements.	Total cost of retired SaaS subscriptions or accounts
Optimized Licensing/Rightsizing Savings	Savings from adjusting license counts or tiers (rightsizing) to match actual, justified usage, particularly for consumption-based models (SaaS/Cloud).	Original License Count/Tier Cost – Optimized License Count/Tier Cost
Consolidation Savings	Savings from consolidating multiple licenses or software versions	Cost of previous licenses – cost after consolidation

B. Cost Avoidance Metrics[80] [81]

[77] https://www.cio.gov/handbook/reporting/fitara-reporting
[78] https://www.gao.gov/assets/gao-24-105717.pdf
[79] The calculation methods and data sources are derived from agency-defined software asset management practices aligned with GAO recommendations and OMB FITARA reporting requirements.
[80] https://files.gao.gov/reports/GAO-25-107041/index.html
[81] https://oversight.house.gov/wp-content/uploads/2017/06/Powner_Testimony_06132017-FITARA-4.0.pdf

Estimates costs avoided by preventing unnecessary purchases or compliance penalties.

Table 4: Example of a Cost Avoidance Metrics

Metric	Definition	Calculation/Data Source[82]
Avoided Overprovisioning Costs	Costs avoided by aligning license counts to actual usage	Number of unused licenses avoided multiplied by cost per license
Compliance Penalty Avoidance	Potential fines avoided by maintaining compliance	Estimated noncompliance fines – actual fines (Zero if compliant)
Procurement Avoidance	Costs avoided by using existing licenses instead of buying new	Cost of new licenses avoided by reallocation
Enterprise Licensing Cost Differential	Costs avoided by using an enterprise agreement compared to a per-user license agreement	Enterprise license cost – Cost per individual license multiplied by number of licenses
Bill Shock Prevention	Potential unexpected financial liabilities avoided by implementing proactive cost anomaly detection and alerting for consumption-based software.	Highest Monthly Spend Anomaly Detected – Agency Approved Monthly Spend
Upgrade/Expansion Avoidance	Costs avoided by extending the life or capacity of existing software or infrastructure through optimization instead of purchasing new.	Cost of Deferred Upgrade or New Infrastructure Purchase

Appendix D: Example of Comprehensive License Inventory

Table 5 lists the data fields that should be included in a comprehensive license inventory, broken down by core,[83] recommended,[84] and optional. These data fields were determined based on findings from GAO reports, FITARA, and M-16-12.

Table 5: Data Fields for Comprehensive License Inventory

[82] The calculation methods and data sources are derived from agency-defined software asset management practices aligned with GAO recommendations and OMB FITARA reporting requirements.
[83] "Core" fields should be captured for every software title.
[84] "Recommended" fields add optimization, life cycle, and governance value.

Category	Data Field	Priority	Definition
License and Entitlement	License agreement number	Core	Agreement or contract reference.
License and Entitlement	Expiration/renewal date	Core	Date subscription or support expires or renews.
License and Entitlement	Quantity purchased	Core	Total licensed quantity acquired.
License and Entitlement	Quantity deployed/assigned	Core	Count currently installed or allocated.
License and Entitlement	Vendor name	Core	Supplier or manufacturer.
License and Entitlement	License type	Core	Perpetual, subscription, term, concurrent, enterprise/site, or open source (See Appendix A).
License and Entitlement	License start date	Core	Effective start date.
License and Entitlement	License term	Recommended	The amount of time the license is available, if it is time-bound.
License and Entitlement	Maintenance/support included	Recommended	Whether support is bundled with license purchase.
License and Entitlement	Entitlement ID/license key	Recommended	Identifier proving licensed rights.
Software Identification	Software title/product name	Core	Primary product name used in inventory and reporting.
Software Identification	Publisher/vendor	Core	Company that owns or publishes the software.
Software Identification	Version	Core	Major version or release tracked for life cycle and support.
Software Identification	Product family/suite	Recommended	Suite or family grouping used for portfolio management.
Software Identification	Edition	Recommended	Edition that affects entitlements and pricing.

Category	Data Field	Priority	Definition
Software Identification	Software category	Recommended	Functional type of software.
Software Identification	Platform	Recommended	Operating systems, browsers, and virtual environments that the platform will be used on.
Software Identification	Build/release number	Optional	Specific build number for patch and support tracking.
Procurement & Contract	Contract number	Core	Award or contract reference.
Procurement & Contract	Purchase date	Core	Date software was purchased or obligated.
Procurement & Contract	Purchase cost	Core	Cost of the license purchase.
Procurement & Contract	Renewal cost	Core	Expected annual or renewal cost.
Procurement & Contract	Contract vehicle	Recommended	Vehicle used to buy the software.
Procurement & Contract	Purchase order number	Recommended	Purchase order or task order reference.
Deployment & Usage	Assigned users/devices	Core	Complete list of users and devices that have been assigned licenses[85]
Deployment & Usage	Installations	Core	Complete list of locations where the software has been installed, including virtual environments and desktop instances.
Deployment & Usage	Business unit/office	Core	Organizations responsible for use.
Deployment & Usage	Last usage date	Core	Most recent verified use date.

[85] This could include nonhuman users, such as a digital worker identity. https://www.idmanagement.gov/playbooks/dw/

Category	Data Field	Priority	Definition
Deployment & Usage	Active user/usage count	Core	Number of users and devices that accessed the software within a specific time horizon (e.g., last 30 days)
Deployment & Usage	Use case justifications	Core	List of all use cases the software is used for.
Deployment & Usage	Install date	Optional	Date software was installed or provisioned.
Infrastructure	Compliance status	Core	Whether current deployment is licensed correctly for each active license.
Infrastructure	Virtualization/cloud platform	Recommended	VMs or cloud environments used to access the software.
Infrastructure	Cloud provider	Optional	Provider if hosted in the cloud.
Compliance & Risk	Approval status	Core	Whether software is approved for use.
Compliance & Risk	Utilization rate	Recommended	Extent to which license is used versus owned.
Compliance & Risk	Audit history/last review date	Recommended	Date of last vendor or internal audit review.
Compliance & Risk	Restrictions/special terms	Recommended	Special rights, limits, or deployment restrictions.
Compliance & Risk	Export/regulatory restrictions	Optional	Restrictions that affect where or how software can be used.
Security and Governance	Business owner	Core	Program or business owner of the software.
Security and Governance	ATO/authorization status	Core	Authorization status if relevant to system use.
Security and Governance	Security risk rating	Recommended	Security or supply-chain risk assessment.
Security and Governance	End-of-support date	Recommended	Date vendor ends support.
Security and Governance	End-of-life date	Optional	Date product reaches end of life.

Category	Data Field	Priority	Definition
Ownership & Accountability	Technical owner/system owner	Core	Technical point of contact responsible for deployment.
Ownership & Accountability	Software asset management/license manager	Core	Individual managing entitlements and compliance.
Ownership & Accountability	Source document links	Recommended	References to agreements, invoices, and vendor terms.
Ownership & Accountability	Contracting officer	Optional	Acquisition POC for renewals and records.
Financial and Life cycle Data	Total cost of ownership (TCO)	Core	All costs associated with the software, including those outside of the license fee, including setup, operations, maintenance, etc.
Documentation	Notes/comments	Optional	Free-form notes for exceptions or context.

Appendix E: CISA CDM Program

The Continuous Diagnostics and Mitigation (CDM) Program, led by DHS's CISA, helps federal agencies continuously secure and gain visibility into their networks and cloud environments. It is essential to clarify that CDM is fundamentally a cybersecurity-focused program, not an IT life cycle management or software or subscription management program. As such, it is not a replacement for an agency's existing IT life cycle management and monitoring program, solutions, or governance.

CDM provides tools, dashboards, and data feeds that let agencies:

- Know what devices and users are on their networks.
- Detect vulnerabilities and misconfigurations.
- Monitor network traffic and risky behavior.
- Track patch status and software inventory.
- Get up-to-date risk scoring and situational awareness.

It is basically a *living security/operations capability*—not a one-time audit.

This table highlights that most capabilities exist in agencies' current tools—often it is just a matter of turning on feeds, connecting APIs, or enabling modules.[86] [87]

CDM Capability Area	Existing Tools Often Already Deployed	Action Needed/"Turn On"	May Require Additional Module/Purchase
Asset Management	Endpoint inventory tools, cloud asset management	Enable inventory reporting into CDM	Rarely; mostly turnkey
Identity & Access Management	AD, Okta, CyberArk, PAM tools	Connect IDP/AD/PAM feeds to CDM	Advanced analytics modules for deeper insights
Network & Perimeter Monitoring	Firewalls, IDS/IPS, proxies, NetFlow sensors	Enable log/API feeds into CDM	Legacy Security Information and Event Management may need connectors
Vulnerability Management	Tenable, Qualys, Rapid7 scanners	Feed scanner data into CDM dashboards	Premium scanning modules for cloud/advanced scanning
Configuration/Baseline Compliance	Endpoint config tools, server hardening software	Turn on baseline compliance reporting	Extended reporting modules if needed
Endpoint Detection/Response	Defender, CrowdStrike, SentinelOne	Enable telemetry/API export to CDM	Cloud/extended modules or extra endpoints licenses
Dashboards/Risk Scoring	CDM Portal	Map existing data feeds	No major purchase; may need setup support

[86] https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-program
[87] https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/mas-it/cdm-tools