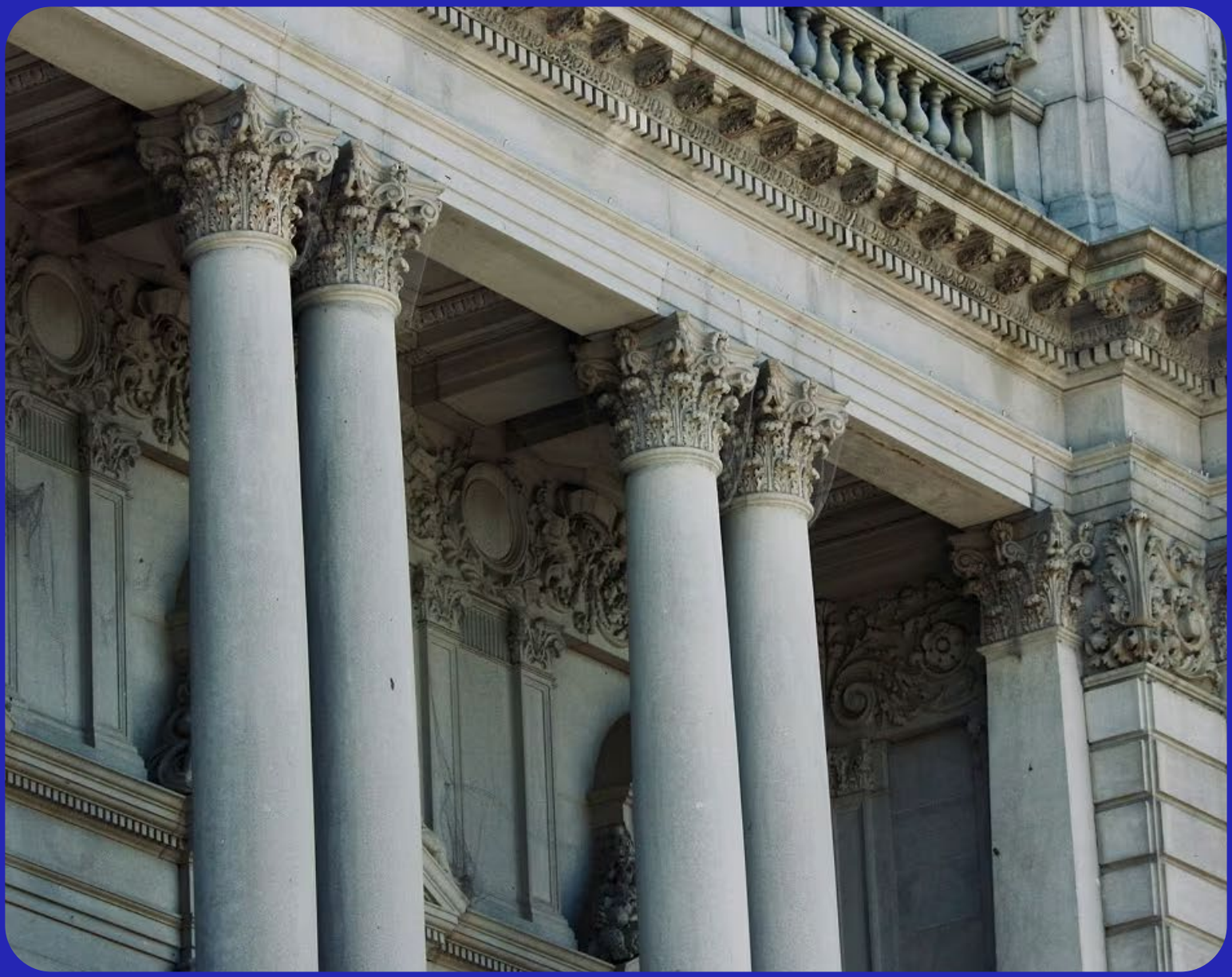


The Cost of Too Many Legal Tools: Why the Government Should Contract Once

EXECUTIVE SUMMARY

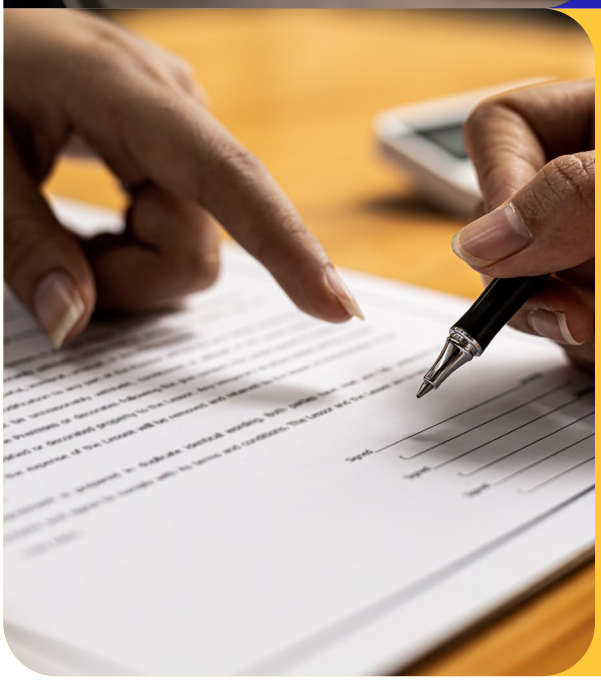
Government Agencies are Struggling To Keep Up: The Multi-Vendor Contracting Problem

Agencies are spending more time and money procuring, learning, and switching between tools than they would if they standardized on a single integrated platform.

Multiple Vendors

- Slow Procurement
- Tool Sprawl
- Inability to Scale
- Additional Employee Training and Turnover
- Higher Cost
- Lower Security

VS



Contracting Once

- Cloud Access and Accessibility
- Unified Platform
- Connectors and Automation
- Highest Level of Security
- Scalability
- Enhanced Accessibility
- Legacy System Integration
- Cost Effectiveness

PART 1

The Challenges of Using Multiple Tools

Complex Procurement Laws, Budget Constraints, and Legislative Complexities

Federal technology procurement remains governed by complex acquisition frameworks such as the Federal Acquisition Regulation (FAR), agency-specific policies, and oversight requirements. The Government Accountability Office (GAO) and the Office of Management and Budget (OMB) have repeatedly noted that lengthy procurement cycles delay modernization efforts and prolong reliance on legacy systems.

According to GAO, federal agencies continue to face delays in modernizing legacy IT because of lengthy acquisition timelines, budget constraints, and risk-averse procurement processes. As a result, technology purchasing cycles routinely extend far beyond those in the private sector, slowing service delivery and increasing costs.

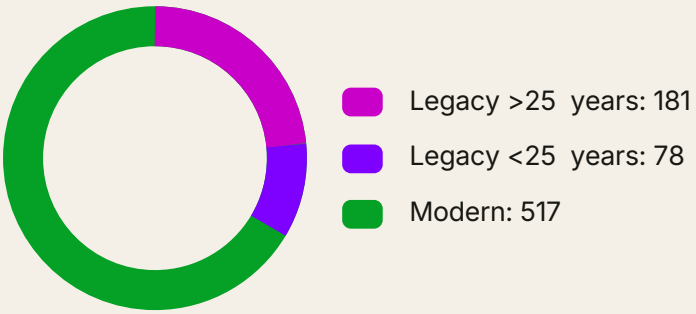
For example, the Internal Revenue Service (IRS) has identified procurement delays as one of the most significant risks affecting taxpayer services and modernization initiatives.[1]

> IRS has acknowledged these legacy assets will continue to contribute to security risks, unmet mission needs, staffing issues, and increased costs.
>
> U.S. Government Accountability Office

The Legacy Challenge: Tool Sprawl and Vendor Fragmentation

Vendor fragmentation, especially with legacy tools, strains agencies on multiple levels. Not only are redundant tools at risk of performing overlapping functions, but integration overload can present a major issue, as systems aren't able to talk to each other as easily as they would under a master contract.

Government agencies have reported using hundreds of outdated tools for day-to-day work. IRS data showed that 259 out of 776 of its applications were legacy tools as of 2022. Out of those, 181 applications were 25 years or older.



Source: Government Accountability Office[2]

Aside from integration issues, tool sprawl also offers an easy path towards overwhelming agency staff. A survey of 2,187 workers in the U.S. and U.K. found that 90% of workers feel overwhelmed by the number of software tools they use, and 75% said that juggling multiple project management tools made it "impossible to get a clear view of work."[3]

Inability To Scale Siloed Systems Causes Delays and Missed Deadlines

Reliance on old technologies like legacy tools or even paper forms can make it impossible to scale systems efficiently — or at all. Even in agencies where paper and pencil is not the norm, siloed systems present integration challenges simply because they are not designed to interoperate.

Lack of unified architecture means agencies wind up maintaining duplicate datasets across multiple applications. Dataset redundancy doesn't just mean duplicated work effort. It can also lead to distorted analytics, inefficient storage, and millions of dollars in annual losses. Even small duplicate rates can translate into thousands of unnecessary records that have to be maintained, reconciled, or cleaned up — a clear symptom of fragmented systems failing to share unified datasets.

53%

The cost of isolation? A 53% service completion delay from government agencies.[4]

Higher Training Costs and Turnover Rates

Companies that reduce complexity see a 40% increase in high performers.[5] That's because more tools often mean a higher training burden and a lower adoption rate, which in turn slows productivity and increases burnout.

Training across multiple tools slows onboarding, increases errors, and reduces productivity. Agencies with fragmented technology stacks also face higher turnover risk, because employees must repeatedly learn new systems.

Legacy platforms compound the problem. Older systems often require specialized expertise, forcing agencies to invest in formal training, extensive documentation, and ongoing retraining that newer hires may never fully absorb.

42% Agreed

"Information at my work is generally too scattered throughout different platforms."

81% Agreed

"I felt overwhelmed with information throughout the onboarding process at my current company."

Source: Glean[6]

The Compounding Costs of Multiple Contracts

IT Procurement Costs

IT procurement is shown to absorb nearly 50% of government agencies' IT budgets. Agencies face higher costs to manage and secure Federal IT investments, largely because they are using siloed systems that perform a singular function.

The Government Accountability Office recently recommended annual IT portfolio reviews,[7] which could save agencies "one hundred million dollars or more in cost savings by reducing duplicative IT investments and halting or terminating investments, when appropriate."

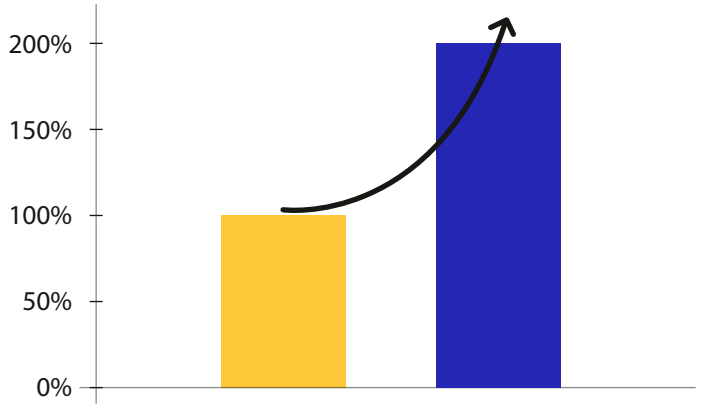
> One hundred million dollars or more in cost savings by reducing duplicative IT investments and halting or terminating investments, when appropriate.

Cost of Maintaining Legacy Systems

Each year, the federal government spends more than $100 billion on IT investments.[8] Agencies have typically reported spending about 80% of that amount on operating and maintaining existing systems, including aging legacy platforms that are costly to maintain and difficult to modernize.

Employee Training and Turnover Costs

Employees lose nearly a full workday — or about seven hours a week — navigating duplicate workflows and fragmented tools.[9] On top of the productivity cost, government agencies must also consider turnover rates. Replacing a government worker can cost up to 200% of the worker's salary, depending on experience and job level.[10] This reflects a number of costs, including recruiting, training, knowledge loss, and service disruption.



Cost of Delays and Missed Deadlines

Requirements evolve during long delays, forcing agencies to redo work they already paid for, as well as being charged by vendors for extended performance periods, change orders, or contract modifications.

Missed deadlines present further expenses, such as required remediation plans, additional reporting, oversight, and compliance costs. In extreme cases, agencies may even face funding restrictions or clawbacks.

Complexity Is the Enemy of Security

Credential Sprawl Leads to Higher Risk of Breaches

Using a host of disconnected tools means more logins, more credentials to manage, and more third-party vendors with some level of access. Password reuse across systems and forgotten or unmanaged accounts also create a level of operational complexity that leaves agencies vulnerable to both human error and malicious attacks.

Fragmented Data Environments Slow Threat Detection

Integrating multiple systems can create vulnerabilities for hackers, as integration gaps create blind spots that act as easy opportunities. A higher number of servers, cloud environments, or endpoints to secure also means a higher number of cybersecurity threats.

Single Platform Organizations Take

72 Days
to detect a security incident

84 Days
to contain one

Source: IBM[11]

Not All Tools Are Built With the Same Level of Security

An industry report on software security maturity shows a significant variation in how different tools are built and maintained at the security level. Forty-five percent of U.S. businesses have reported that they stopped using certain software because of security risks.[12]

As of October 2025, the list of breaches included hundreds of CVEs across Windows, Cisco, Oracle, and other similar systems.

In 2025 alone, tens of thousands of new software vulnerabilities were recorded, with thousands of new CVEs (Common Vulnerabilities and Exposures) disclosed every month.

100
breaches disclosed by government agencies in 2023.

35%
more breaches than the previous year.

Source: Deepstrike[13]

PART 2

The Solution to Overly Complex Agency Infrastructure? Contract Once

Cloud Access and Accessibility

Cloud migration offers a solution to just about every challenge we've seen so far. Federal initiatives such as the Cloud Smart Strategy and Zero Trust mandates emphasize secure, scalable cloud adoption to reduce legacy system dependency and improve mission delivery.

Cost Savings:
Lower initial investment, reduction of unpredictable expenses, and lower long-term maintenance costs

Improved Security:
Enhanced protection through security features like encryption, multi-factor authentication, and compliance certifications

Faster Delivery:
Quicker interagency communication and deployment of mission-critical solutions, even for tight deadlines that involve complex datasets

Scalability:
Ability to adapt to changing requirements and scale resources on demand

Regulatory Compliance:
Government-specific regulation adherence

Cost, Risk, and Performance

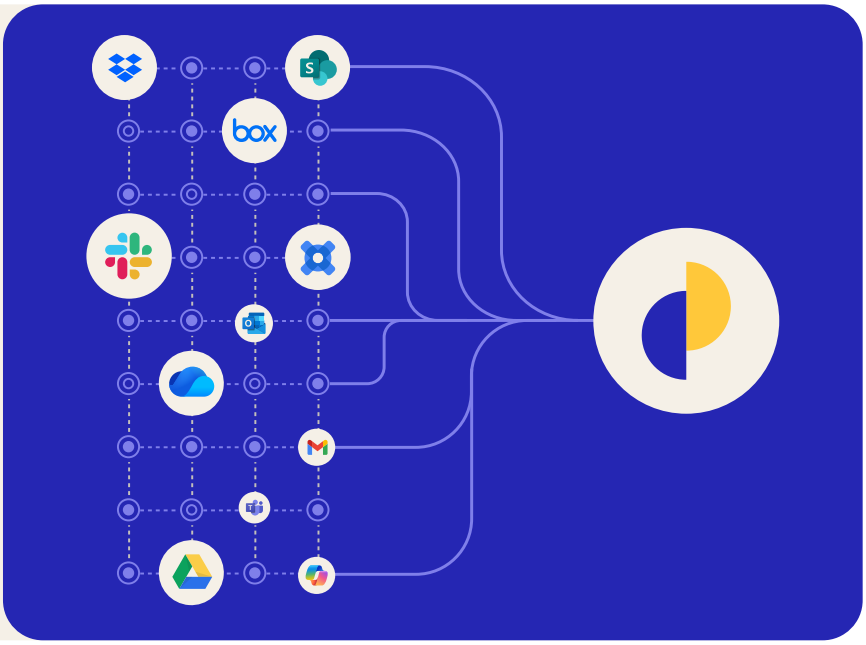
Multi-Vendor	VS	Unified
Complex Procurement **Multiple tools mean multiple contracts, approvals, and renewals.** *Example: An agency spends over a year procuring separate FOIA, eDiscovery, and legal hold tools*	Cost	**Streamlined Acquisition** **One platform simplifies contracting, renewals, and vendor management.** *Example: The same agency acquires a single platform covering all workflows under one contract, reducing time and overhead.*
Fragmented Security and Compliance **Each tool adds compliance gaps, and security is only as good as the weakest link.** *Example: As data moves between systems, it requires manual documentation to maintain chain of custody and audit readiness.*	Risk	**Consistent End-to-End Controls** **Platform- and company-wide credentials that span all workflows.** *Example: All data is processed within a FedRAMP® Moderate/High and DOD IL5/IL6 Authorized environment, with automated audit logs across the lifecycle.*
Interrupted Processes **Performance slows as data is exported, re-ingested, and re-processed between tools.** *Example: A FOIA team exports records for redaction and waits for them to be processed again before review can continue.*	Performance	**Shared Processing Power** **Discovery, review, and compliance workflows run on a single, scalable platform.** *Example: Records ingested for a FOIA request are immediately available for analytics, AI-assisted review, and automated redaction, without moving data to another system.*

Connectors and Automation

A secure, streamlined data collection process can significantly lower delays in service and helps teams to manage complex and disparate data types. By seamlessly connecting applications, cloud-based data repositories, collaboration tools, and email databases all in one organized setting, you are one step closer to eliminating the need for multiple tools.

A Unified Platform

One sweeping solution to the aforementioned problems is a unified, end-to-end platform. As we saw in Part 1, organizations using a unified cybersecurity platform detect incidents 72 days faster and contain them 84 days faster than organizations relying on disparate tools. That means higher security while you manage complex needs at the most sensitive level.



Highest Level of Security

Rather than risking security breaches with sprawling credentials and fragmented data environments, a single contract will reduce silos and lead to higher security across the board. This is especially crucial in the government sector, where security breaches affected roughly 15 million individuals in 2025.[13]

Every additional vendor introduces another authentication layer, another integration bridge, and another set of security controls to manage. Unified platforms don't just multiply efficiency — they significantly lessen agencies' attack surface.

Potential Entry Points for Attackers	Unified Platforms Consolidate These Into
More Log-in Portals	Fewer authentication endpoints
More Databases	Fewer integration pathways
More API Connections	Fewer patch cycles
More Patches/Updates	Fewer exposed databases
Different encryption standards	Standardized encryption standards
Different compliance certifications	One compliance framework (e.g., FedRAMP® alignment)
Sprawling Credentials	Centralized Authentication (SSO)

Scalability

Siloed systems force agencies to add new point solutions every time requirements grow, such as with new compliance mandates or new data types. A scalable platform manages these requirements by efficiently handling increased complexity, adding new modules without introducing new vendors, and expanding functionality without replacing the core system.

Scalable platforms also have the advantage of reducing security risks, since integrations are built-in, and APIs and access controls are centralized. This results in lower maintenance costs and fewer security blind spots.

A secure platform should be especially well equipped to scale alongside large and diverse datasets. Government clients specifically benefit from a platform that reviews and processes multiple complex data types, especially with the growing number of FOIA requests for a wide range of data such as audio files, chat logs, and body camera footage. Cloud eDiscovery enables seamless scaling as data volumes and user demands evolve — a core advantage over legacy systems that struggle with exponential data growth.

Enhanced Accessibility

Another significant benefit of single contracting is that collaboration and data access become more accessible across teams, including remote teams. The cloud allows seamless collaboration and real-time data sharing, so communication delays are kept to an absolute minimum. With a unified, collaborative platform, authorized users are able to securely access necessary information anytime from anywhere in the world.

Legacy System Integration

Most agencies operate on 10- to 30-year-old databases that rely on custom-built internal applications. These outdated systems hold critical data, such as case files, personnel records, legal hold data, and financial records. Without a platform that integrates legacy system data, agencies will have to rely on manually migrated data — that means duplicate datasets, security risks, and version control problems.

It's important to find a vendor that can integrate existing tools and workflows, all while moving core infrastructure into a more collaborative, secure, and cost-effective data landscape. As agencies modernize away from outdated, siloed software, seamless legacy system integration means less risk, higher security, and a lot less stress for employees and leaders.

Cost Effectiveness

Unified platforms present a number of cost-saving measures, including reduction of duplicate tools and services, lower employee training costs, and faster service delivery times (lessening the financial burden that comes with delays and missed deadlines). IT costs are also lowered when using cloud-based systems, as there is no expensive hardware or maintenance for IT teams to manage.

Another significant advantage of contracting once is that you'll often receive a simple, transparent pricing model. With one comprehensive pricing model, agencies will have access to all major features within one platform, instead of being charged piecemeal for multiple modules or add-ons — a common cost driver for fragmented tool stacks.

Multiple Vendor Costs	Single Contractor Costs
Separate subscription for each vendor (often with overlapping features)	One subscription that bundles multiple capabilities
Cost to build and maintain connectors/APIs between systems	Minimal or included integrations — fewer external integrations needed
Training for each distinct tool (different UX, workflows)	Single training curriculum for one platform
Multiple support contracts, differing SLAs, redundant vendor management	One support contract with unified SLA & central help desk
Individual security assessments, patch cycles, and audits per vendor	Centralized security controls — one audit cycle, unified compliance

Conclusion

Modernization starts with decluttering your toolset.

There was a time when multiple vendors were necessary. Fortunately, that is no longer the case. The emergence of powerful all-in-one platforms gives agencies the opportunity to boost efficiency, security, and overall performance while reducing timelines, costs, and employee fatigue.

It's time to simplify your tech. And for government agencies, that means finding a trustworthy vendor to handle complex data at the highest level of efficiency and security. As a highly trusted data environment, Casepoint offers the tools necessary to modernize – seamlessly, securely, and all in one place.

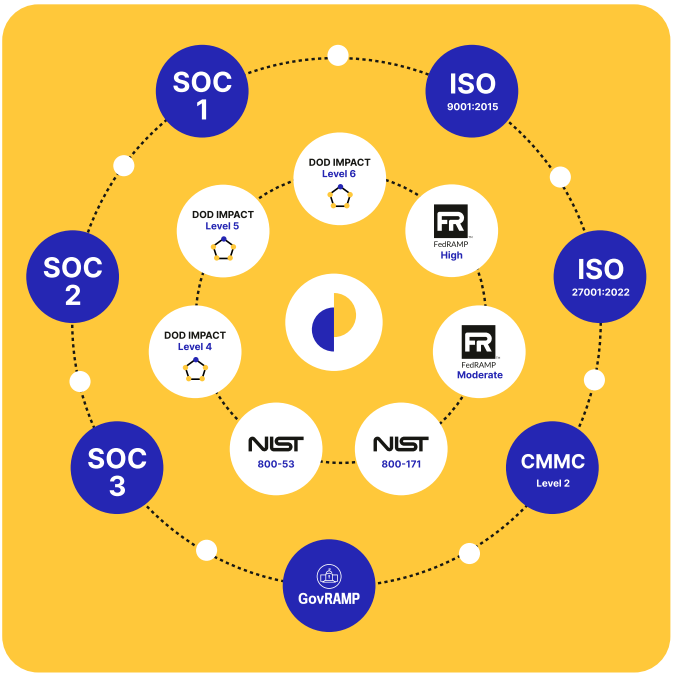
References

1. Taxpayer Advocate Service, 2025 Annual Report to Congress: https://www.taxpayeradvocate.irs.gov/reports/2025-annual-report-to-congress/full-report/
2. GAO, IRS Needs to Complete Modernization Plans and Fully Address Cloud Computing Requirements: https://www.gao.gov/products/gao-23-104719t
3. Quickbase, Inside the 2025 Gray Work Report: https://www.quickbase.com/blog/inside-the-2025-gray-work-report-investment-in-productivity-tech-is-up-productivity-not-so-much
4. European American Journals, Breaking Down Data Silos: https://eajournals.org/ejcsit/vol13-issue48-2025/breaking-down-data-silos-how-ai-builds-bridges-in-the-cloud/
5. Consultport, The Hidden Cost of Organizational Complexity: https://consultport.com/business-excellence/organizational-complexity-and-how-to-fix-it/
6. Glean, 2023 Onboarding Survey Report: https://www.glean.com/resources/guides/onboarding-survey-ebook
7. GAO, 2025 Annual Report: https://www.gao.gov/products/gao-25-107604
8. GAO, Agencies Need to Plan for Modernizing Critical Decades-Old Legacy Systems: https://www.gao.gov/products/gao-25-107795
9. Freshworks, The Cost of Complexity on Business: https://www.freshworks.com/theworks/employee-experience/cost-of-complexity-report-blog/
10. Munitemps: Hidden Employee Turnover Costs: https://www.munitemps.com/2025/09/04/hidden-employee-turnover-costs-the-public-sectors-silent-budget-killer/
11. IBM, Capturing the Cybersecurity Divide: https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/unified-cybersecurity-platform
12. Gartner, Why Security Is a Priority for Software Buyers in 2024: https://www.gartner.com/en/digital-markets/insights/2024-buying-trends-software-security
13. Deepstrike, 2025 Vulnerability Statistics: https://deepstrike.io/blog/vulnerability-statistics-2025

What's Next?

How Casepoint Can Help

It can seem like a major overhaul, but a good all-in-one platform makes it easy to replace your current multi-tool system. Especially when you choose a partner with user-friendly experience complete with training resources and on-call customer support. With Casepoint, you get an experienced government team that is trusted by top U.S. agencies. Casepoint allows agencies to manage litigation, legal holds, investigations, data privacy, AI-assisted reviews, FOIA requests, and congressional inquiries — all in one place.



About Casepoint

Casepoint delivers comprehensive legal and compliance software that enterprises and government agencies rely on to manage their most critical workflows. Serving large corporations, major federal agencies, and the Department of War, Casepoint automates litigation readiness, powers litigation and investigations, simplifies FOIA management, and supports regulatory compliance. Built on Casepoint's award-winning data discovery platform and industry-recognized customer partnership model, the company combines purpose-built solutions with AI and advanced analytics. Its security posture includes FedRAMP® High and DOD Impact Level 5 (IL5) and IL6 authorizations, helping legal and compliance teams work faster, reduce risk, and make confident decisions.

See how a unified platform with best-in-class security can transform your agency's workflows.

Connect With Us

casepoint

casepoint.com

hello@casepoint.com

+1 (844) 882-0021