IT Is Not a Commodity:

Delivering Mission Value Through the Federal Supply Chain

How the federal IT market delivers innovation, security, and competition that drive mission success.

Prepared by Tony Celeste

Executive Director & General Manager, Ingram Micro Public Sector LLC

October 2025

The views expresed in this document refect the author's professional perspective and do not necessonily represent the official position of Ingram Micro Inc. or its afiliates.

Executive Summary:

IT is not a commodity. Almost every solution requires integration, compliance, and mission alignment.

Policymakers and acquisition leaders are increasingly treating information technology as if it were interchangeable commercial goods, like pens or paper. Some of this thinking has its roots in category management, which groups diverse IT offerings together and assumes they are essentially the same. This oversimplification is reflected in efforts such as OMB and GSA's pursuit of centralized price negotiations and centralized acquisition initiatives. These efforts are based on a false assumption that intermediaries such as distributors, Information Technology Value-Added Resellers (ITVARs), and systems integrators add limited advantage, while charging significant markups that only drive higher long-term costs.

This paper examines how government-unique security, compliance, and supply-chain requirements transform commercial technology into mission-conditioned solutions, and why that reality matters for pricing, competition, and long-term value.

The reality is vastly different. The federal IT ecosystem, including Original Equipment Manufacturers (OEMs), distributors and aggregators, ITVARs, and prime contractors, provide critical services that help government acquire secure, compliant, affordable, and mission-ready solutions. Attempting to strip out these functions or force direct-only OEM transactions risks solution lock-in, reduced market choice, stifled innovation, and higher costs over time.

This paper highlights the unique benefits that each participant in the federal IT market provides, with particular emphasis on distributors, and explains why preserving this diverse market structure is essential for mission success and U.S. global competitiveness.

Problem Statement: Mischaracterizing IT as Commodity

OMB and GSA are increasingly treating IT as simple commodity COTS (Commercial Off-the-Shelf) items, ignoring the complexity of integration, compliance, and lifecycle support. This posture is reflected in initiatives such as ONEGov centralized negotiations and other centralized acquisition efforts, many of which have their roots in category management. By grouping diverse IT offerings into broad categories and assuming they are interchangeable, these approaches oversimplify how IT is bought and delivered.

These initiatives are not without merit. Efforts to provide greater visibility into IT spending and to identify areas of overlap across agencies can improve efficiency and reduce unnecessary duplication. However, they risk going too far by oversimplifying IT solutions as interchangeable commodities rather than recognizing their complexity and mission specificity.

This oversimplification weakens the federal IT market structure that supports diverse participation, small business involvement, competition, and the integration of OEM technology into mission-specific solutions. It also penalizes vendors that invest billions of dollars in research, development, and compliance with the government's unique requirements. In doing so, it can discourage innovation or at a minimum deemphasize its importance as a driver of modernization and mission outcomes across the public sector.

Original Equipment Manufacturers (OEMs): Innovation Engines

Original Equipment Manufacturers are the technology innovators of the federal IT market. They design and deliver the hardware, software, cloud platforms, and cybersecurity tools that drive government modernization. From artificial intelligence and machine learning to high performance computing, to cloud infrastructure and networking, OEMs bring the breakthroughs that enable federal agencies to transform mission operations.

The government benefits from this technological advancement, but OEMs by themselves are not sufficient to deliver mission-ready solutions. Each OEM can only promote its own catalog, and the incentive is to sell more of its own products rather than identify the best mix of technologies for an agency's mission. When government relies on OEMs directly, it risks narrowing its choices to a single brand or incumbent supplier.

Government Contribution: OEMs provide the innovation foundation, but without the broader federal IT market, agencies risk limited choice, technology lock-in, and solutions that may not fully align with mission requirements. The supply chain ensures new capabilities are delivered in ways that are compliant, secure, and mission-ready.

Distributors and Aggregators: The Backbone of the Federal IT Delivery Network

Distributors are sometimes misunderstood as intermediaries that simply move products from vendors to ITVARs. In reality, they are the backbone of the federal IT delivery network and provide far more than logistics. They secure product authenticity, finance transactions, enable partners, and orchestrate the delivery of technology in ways government could not cost effectively replicate on its own. Their role is essential for making IT accessible and mission-ready across government.

A core function of distribution is supply chain integrity and compliance. Distributors safeguard product authenticity, prevent counterfeit or unauthorized items, and manage compliance with federal standards including FAR, DFARS, ITAR, EAR, CMMC, and insider threat programs. These requirements extend beyond OEMs and apply throughout the delivery chain, meaning distributors, ITVARs, and systems integrators must also meet federal safeguarding, sourcing, reporting, and cybersecurity standards. They maintain secure warehousing and logistics so that technology solutions can be delivered even to sensitive or classified facilities, protecting agencies from mission disruption and cyber compromise.

Distributors also provide credit, financing, and risk absorption. Many small ITVARs and even larger prime contractors cannot carry federal receivables that may take 90 to 120 days to be paid.
Distributors extend credit and absorb that risk, allowing these companies to compete for and perform on federal contracts. They also provide leasing and consumption-based models that align with the government's OPEX versus CAPEX funding structures. By lowering these barriers to entry, distributors empower entrepreneurial and innovative small businesses to bring forward novel solutions for federal missions. This not only helps agencies meet socio-economic goals but also broadens the range of transformative technologies and approaches available to government. In doing so, distributors reinforce the federal, defense, and U.S. industrial base by ensuring that technological advancement from emerging firms can scale into mission-ready solutions.

Another critical function is aggregation and contract access. By consolidating hundreds of OEM relationships into a single channel, distributors simplify procurement and reduce costs for government and its partners. They provide access to key contract vehicles such as GSA MAS, NASA SEWP, Army ITES-4H, and NIH NITAAC CIO-CS, all designated Best-in-Class (BIC) by OMB. In doing so, they also absorb costs tied to other contract terms such as shipping and logistics (FOB destination), inspection and acceptance requirements, and reporting obligations. This aggregation makes competition real and accessible while relieving government of significant administrative burden.

In addition, distributors provide market intelligence, accelerate modernization, and support sustainability. They track demand trends, product availability, and emerging technologies, giving agencies and partners the data needed for smarter and faster acquisition decisions. Distributors also help emerging OEMs enter the federal market more quickly than direct sales models allow, expanding open market participation and increasing access to new capabilities. They provide lifecycle support such as secure asset recovery, recycling, and environmentally compliant disposal, aligning with government sustainability and climate objectives.

Beyond these direct benefits to government, distributors strengthen the broader federal IT marketplace by enabling ITVARs and prime contractors. This includes providing technical training, certifications, pre-sales engineering, marketing support, and compliance guidance. Distributors also drive demand generation and proof-of-concept activities while offering services such as imaging, kitting, and refresh programs. These capabilities expand the capacity of small businesses, ITVARs, and systems integrators, giving agencies a deeper and more capable supplier base.

For OEMs, distributors represent a lower cost of sale by managing logistics, training, and partner enablement on their behalf. This allows vendors to extend their reach into niche agencies and specialized markets without the overhead of building direct sales and support operations. The efficiencies created by distribution ultimately lower the cost of technology for government and make solutions more affordable.

Finally, distributors provide resilience and orchestration. They maintain geographically distributed warehouses and logistics hubs to enable continuity of supply during emergencies, natural disasters, or geopolitical disruptions. Distributors also orchestrate multi-vendor solutions by validating interoperability and preconfiguring bundles so agencies can adopt secure, integrated capabilities more quickly. These capabilities increasingly intersect with the integration, configuration, and solution-enablement work performed by ITVARs and systems integrators, reinforcing the complementary and interdependent nature of the federal IT supply chain. Taken together, distributors function as vendor-neutral advisors whose independence drives competition, prevents solution lock-in, and broadens the range of innovative technologies available to support government missions.

Government Impact: Distributors provide the foundation for a secure, resilient, and dynamic IT marketplace. Beyond logistics, they deliver supply chain integrity, compliance assurance, financing, cybersecurity alignment, market intelligence, lifecycle sustainability, surge capacity, and vendor-neutral advice. They enable small and diverse firms, reduce OEM costs, and orchestrate multi-vendor ecosystems so government can access secure, affordable, and mission-ready technology at scale.

IT Value-Added Resellers (ITVARs): Trusted Advisors and COTS-Focused Prime Contractors

ITVARs serve as trusted advisors and, in many cases, as prime contractors focused on delivering commercial off-the-shelf (COTS) technology solutions. Their role is to install, integrate, and tailor these solutions to the specific mission needs of federal agencies. They complement the role of the large systems integrators, by ensuring agencies not only acquire the right technologies but also receive the value-added services that make those technologies effective in mission environments.

The strength of ITVARs lies in their ability to provide mission-specific customization and services around COTS solutions. They configure hardware and software, integrate systems, provide user training, and often deliver managed services such as cybersecurity monitoring, patching, and Tier 1 and Tier 2 help desk support. In doing so, they make sure that agency IT solutions are not only compliant with federal requirements but also aligned to the specific operational context of each mission. By tailoring COTS solutions to unique mission requirements, ITVARs help agencies turn commercial technology into mission-ready capability. These support capabilities are critical in federal environments where agencies rely on timely, secure, and compliant assistance to maintain continuity of operations and user readiness. While ITVARs can leverage the foundational work distributors perform, many also deliver overlapping capabilities in integration, configuration, compliance preparation, and managed services. These complementary roles strengthen the delivery chain by expanding on distributor groundwork and providing the last mile of mission-tailored solutions agencies rely upon. Yet they are often overlooked in acquisition planning, despite being essential to sustaining mission performance and ensuring that deployed technologies remain fully operational and compliant throughout their lifecycle.

Many ITVARs operate as prime contractors on federal opportunities, particularly where requirements are focused on delivering technology solutions rather than developing new mission platforms. Their work is distinct but complementary to that of the large systems integrators, which build and sustain highly complex, custom-engineered systems such as military command-and-control systems, weather monitoring infrastructure, advanced sensor and satellite networks, and national air traffic control systems. ITVARs, by contrast, excel in delivering value-added, COTS-based solutions that strengthen and enable these larger mission platforms.

ITVARs also carry a heavy burden of compliance and certification, maintaining staff and infrastructure to meet federal requirements such as CMMC, FISMA, and export controls. Agencies benefit from this compliance capability without having to absorb those costs internally.

Many ITVARs also deliver engineering, integration, and lifecycle services that overlap with and complement the work of distributors and systems integrators, creating a more capable and resilient delivery chain for commercial off-the-shelf technologies in federal missions.

Finally, ITVARs play a vital role in meeting socio-economic contracting goals. Many are 8(a), Women-Owned Small Businesses (WOSB), Service-Disabled Veteran-Owned Small Businesses (SDVOSB), or HUBZone firms. By participating in the federal market, they advance government's statutory objectives for small business utilization and safeguard a more diverse, resilient supplier base.

Government Contribution: ITVARs are critical to delivering the last mile of mission enablement. As prime contractors for COTS-based technology solutions, they install, integrate, and tailor IT to agency missions while complementing the work of major systems integrators. Their independence and vendor-neutral approach expand competitive choice, advance modernization, and strengthen the diversity and resilience of the federal IT supply chain.

Prime Contractors and Major Systems Integrators: Delivering Mission-Critical Platforms and Outcomes

Together, ITVARs and large systems integrators form a connected delivery chain that transforms commercial technology into mission platforms. Where ITVARs focus on tailoring COTS solutions for specific agency needs, systems integrators extend that work to engineer, integrate, and sustain the large-scale platforms that enable national missions.

Prime contractors, particularly the large systems integrators (SIs), provide the scale, resources, and expertise required to design, build, and sustain some of the government's most complex and mission-critical systems. They serve as the lead contractors on enterprise-level programs, that often span decades and involve billions of dollars in investment. Their role is distinct from, but complementary to, that of ITVARs. While ITVARs focus on delivering commercial off-the-shelf (COTS) technology and related services, SIs are responsible for integrating those technologies into the broader mission platforms and infrastructures that underpin national security and public safety.

Large systems integrators bring together diverse technologies from OEMs, distributors, and ITVARs to deliver custom-engineered platforms that are central to national missions. These include military command-and-control systems, weather monitoring and forecasting platforms, advanced sensor and satellite communication networks, and the nation's air traffic control infrastructure. These platforms are not off-the-shelf purchases; they require years of engineering, integration, testing, and sustainment to meet government's unique mission requirements and operational standards.

Beyond designing and delivering these platforms, SIs provide extensive operational support and mission expertise. They operate and maintain mission systems, provide cleared personnel, and manage critical functions that ensure government missions run effectively. They bring program management discipline, systems engineering capability, and deep understanding of agency missions. In doing so, they deliver not only technology platforms but also continuous mission assurance.

Many of the services provided by systems integrators overlap with and depend on the foundational work done by distributors and ITVARs, reinforcing the fact that the entire delivery chain must operate together for agencies to receive secure, integrated, and mission-ready solutions.

SIs also depend on the broader federal IT market to succeed. For success, they rely on distributors for secure and compliant access to technology, on OEMs for new technological capabilities, and on ITVARs and small businesses for specialized services and localized mission expertise. Acting as the integrators of the supply chain, SIs weave together these diverse capabilities to create resilient and interoperable solutions that meet government's most demanding mission needs.

Government Benefit: Systems integrators deliver enterprise-scale platforms and operational support that agencies depend on to fulfill their missions. They combine COTS technologies with custom engineering, program management, and mission expertise to create solutions that are secure, resilient, and tailored to national requirements. By leveraging the full breadth of the federal IT market, they enable mission assurance, foster innovation, and maximize return on investment for taxpayers.

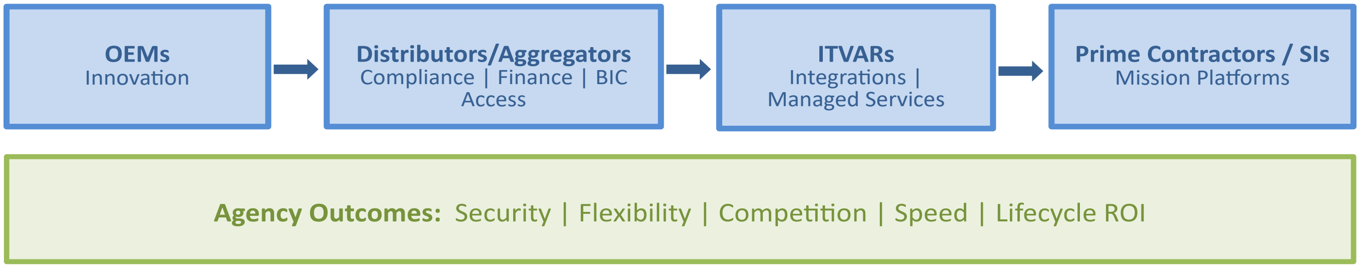
OEMs
Innovation
Distributors/Aggregators
Compliance | Finance | BIC Access
ITVARs
Integrations | Managed Services
Prime Contractors / SIs
Mission Platforms
Agency Outcomes: Security | Flexibility | Competition | Speed | Lifecycle ROI

Figure 1: Federal IT Supply Chain and Mission Outcomes

Why IT is Not a Commodity

Despite its widespread use, information technology is not a commodity. Every federal IT solution requires integration, compliance, and alignment to specific mission requirements. Treating IT as if it were interchangeable overlooks the investments, certifications, and unique capabilities that differentiate products and services in this market.

The commercial technology industry invests hundreds of millions to billions of dollars annually in research and development to deliver new capabilities and drive modernization. Just because a technology product is widely used does not mean it is interchangeable. Consider smartphones: both the iPhone and Android devices are categorized as smartphones, but they are not commodities. Each offers distinctive features, operating systems, and user experiences. Federal IT is the same. Two cybersecurity platforms or two cloud services may fall under the same category, but they are designed and supported very differently, with varying capabilities that directly affect mission outcomes.

Federal IT also comes with unique requirements that add cost and complexity well beyond commercial markets. For example, laptops purchased by government often require built-in CAC readers for multifactor authentication, a feature almost no commercial company would use.

Federal solutions must also comply with standards such as FIPS encryption, FedRAMP cloud authorization, FISMA, JITC certification, Common Criteria evaluations, and CMMC requirements. Products may need to be manufactured in the United States under Trade Agreements Act (TAA) compliance, and personnel supporting them may require security clearances. These requirements exist to protect national security and sensitive information, but they also introduce operational and compliance obligations that do not exist in the commercial sector.

Even when technologies originate as commercial products, federal requirements such as cryptographic validation, continuous security governance, authorization processes, sourcing restrictions, and safeguarding obligations fundamentally change how those technologies are engineered, deployed, operated, and sustained. These mandates add real and recurring costs that do not exist in the commercial market, yet acquisition policy often continues to benchmark pricing as if those costs were not present.

Centralized visibility into what agencies are buying can be valuable for identifying overlap and eliminating waste. At the same time, it must be balanced against the reality that some duplication is intentional. Agencies often maintain parallel systems to provide redundancy and deliver mission resilience. Eliminating this kind of duplication would jeopardize operational continuity rather than create savings.

Yet government procurement often assumes the opposite: that because it buys at scale, it should pay less than commercial customers. In reality, the model is reversed. Federal customers demand more features, greater security, and stricter compliance than commercial buyers. Instead of being asked to reduce IT product costs, industry should be fairly compensated for meeting these additional demands. Ignoring these realities and imposing arbitrary price controls penalizes vendors for delivering exactly what agencies require and limits their ability to continue investing in new technologies.

Government Outcome: Recognizing IT as a differentiated, mission-critical capability ensures that agencies pay a fair price for the added requirements they impose. It also preserves the incentives for industry to keep innovating while ensuring that government continues to receive secure, compliant, and modern technology tailored to mission needs. Treating IT as a commodity may create short-term cost pressure, but it ultimately reduces flexibility, discourages innovation, and increases long-term lifecycle costs for taxpayers while eroding mission readiness, security, and U.S. global competitiveness.

Policy Question for Consideration

Federal IT hardware, software, cloud, and services are legally classified as commercial items under the Federal Acquisition Regulation (FAR). Yet in practice, they must meet mandatory government-unique requirements for security, compliance, sourcing, and ongoing authorization and lifecycle support that do not exist in the commercial market.

Given these realities, on what basis should federal acquisition policy expect pricing at or below purely commercial market levels, and how should policy evolve to account for the true cost and value of delivering secure, compliant, and mission-ready technology?

Solutions vs. Parts: An Automobile Analogy

Federal IT acquisitions are too often approached as if the government were buying individual parts rather than complete solutions. Policymakers focus on negotiating the unit price of a server, software license, laptop, or network switch while overlooking the value of the integration, compliance, and lifecycle support that make those components function together as a mission-ready system.

A useful analogy is the automobile. The federal IT market is more like a car than a collection of parts. A vehicle’s value comes from how its tires, brakes, engine, and transmission are designed, assembled, and tested to work together safely, not from each part priced in isolation. Its usefulness lies in how those parts are integrated, assessed, and supported to function as a safe and reliable vehicle. No one would suggest pricing the car by dictating what each component should cost, ignoring the labor, engineering, safety certifications, and warranty protections that make it whole. Yet this is precisely what happens when government tries to remove distributor, reseller, or integrator services and focuses only on the OEM product price.

In reality, IT is delivered as solutions, not parts. Every deployment requires configuration, compliance validation, cybersecurity hardening, and ongoing support. Distributors absorb the financial and compliance risk; ITVARs provide integration and training; and systems integrators combine multiple OEM technologies into mission-critical platforms. Attempting to separate these elements and dictate prices for individual parts disregards the significance of the work that makes the system effective for government missions.

Government Value: Viewing IT as complete solutions rather than interchangeable parts supports the delivery of secure, compliant, and mission-ready systems. Ignoring this reality may appear to generate savings but ultimately reduces capability, increases lifecycle costs, and delays mission outcomes. Recognizing the full impact of integration and support protects taxpayer investment and strengthens mission performance.

When IT is treated as a collection of parts rather than an integrated solution, it often leads to policies that prioritize direct purchasing from OEMs at the expense of competition and benefit. The next and most significant risk emerges when government seeks to bypass the broader ecosystem of providers altogether and negotiate directly with incumbent manufacturers.

Risks of Direct OEM Negotiations

In an effort to demonstrate cost savings for taxpayers, government has increasingly pursued direct negotiations with incumbent OEM vendors. Although this approach may appear to lower prices in the short term, it creates risks that reduce competition, limit choice, slow technological progress, and increase long-term costs for federal missions.

The first risk is the creation of brand or solution preference that leads to lock-in. When agencies negotiate directly with OEMs already in use, they effectively endorse those vendors as preferred suppliers. This narrows choices, discourages consideration of emerging solutions, and reduces the government's ability to evaluate competing technologies. Over time, it limits flexibility and erodes competitive pressure in the market.

The second risk is slower innovation and reduced access to emerging technologies. New and smaller OEMs often rely on distributors and ITVARs to reach the federal market. Bypassing these intermediaries cuts off the pathways that surface new technologies, particularly from entrepreneurial and diverse suppliers. The result is fewer opportunities for agencies to adopt modern, mission-enhancing capabilities that might better meet their needs while delivering better performance, lower costs, or stronger cybersecurity.

A third risk is the creation of barriers to entry for small businesses. Many small and disadvantaged firms depend on distributors for credit, contract access, and compliance support. When government works directly with OEMs, these businesses are excluded from participation, reducing supplier diversity and weakening the industrial base that supports federal missions.

Finally, direct OEM negotiations create unintended lifecycle costs. Without the advisory services, integration support, and compliance oversight that the broader IT market provides, agencies risk acquiring isolated products rather than complete, mission-ready solutions. The hidden long-term costs of integration delays, system incompatibility, and reduced flexibility often outweigh any short-term savings achieved through direct negotiations.

Government Value at Risk: Direct OEM negotiations may seem to save money, but they reduce competition, limit flexibility, and weaken the innovation pipeline that drives mission outcomes. The federal IT supply chain delivers benefit through integration, compliance, financing, and risk management. Strengthening this ecosystem ensures agencies receive the best technology, the strongest industrial base, and the greatest long-term return for taxpayers.

Recommendations

For federal IT procurement to deliver secure, innovative, and affordable mission outcomes, policymakers must move away from treating IT as a simple commodity. While the government often classifies information technology as "commercial off the shelf" (COTS), the solutions it purchases are not truly commercial in practice. Federal requirements for security, compliance, packaging, shipping, delivery, and lifecycle support transform COTS products into uniquely governed solutions with added cost and complexity. Recognizing this distinction and the full contribution delivered by the broader market is essential to achieving mission readiness and value for taxpayers. Several policy actions can help achieve this balance.

Recognize IT as mission-critical, not commodity. Federal acquisition policy should acknowledge that IT solutions require integration, compliance, and mission alignment. Every purchase is more than an IT product; it is part of a larger system that enables national security, public safety, and citizen services. Policies that reduce IT to a commodity risk increasing lifecycle costs and diminishing mission performance.

Strengthen free market competition. Arbitrary markup caps and direct OEM negotiations distort pricing and reduce flexibility. A vibrant market of choices is the most effective mechanism for controlling cost while preserving access to the advisory, compliance, and integration capabilities that government relies upon. Market-driven pricing encourages investment in new capabilities, accountability, and value-for-money outcomes for taxpayers.

Encourage open standards, not brand preference. Instead of reinforcing incumbent vendors through direct negotiations, government should focus on adopting open industry standards that promote interoperability. This approach expands choice, fosters competition among multiple suppliers, reduces lock-in, and accelerates technological advancement to the benefit of mission outcomes.

Support the role of distributors and entire IT supply chain as a national asset. Distributors, ITVARs, and systems integrators extend OEM technological capabilities to every level of government. They provide compliance assurance, supply chain security, small business enablement, and risk management. Strengthening this ecosystem sustains the federal and defense industrial base, ensures resilience in times of crisis, and maintains U.S. leadership in technology and innovation while providing IT alternatives and safeguarding against solution lock-in.

Promote balance in centralized acquisitions initiatives and category management. Efforts to gain visibility into IT spending are important, but centralized price setting or one-size-fits-all contract models can create unintended consequences. Visibility should be paired with flexibility, enabling agencies to procure technology that meets unique mission needs while maintaining accountability and transparency. Grouping all IT solutions into broad categories and treating them as interchangeable creates a false sense of uniformity. Information technology is diverse and complex, and these characteristics should be recognized in acquisition policy. Policymakers should ensure that category management and centralized acquisition initiatives account for this diversity and do not inadvertently reduce choice, competition, or innovation.

Ensure government pays fair value for what it requires. Federal customers impose unique requirements such as FIPS, FedRAMP, JITC, CMMC, TAA compliance, CAC readers, and cleared support personnel. These mandates add real cost and complexity for industry partners. Rather than assuming government should always pay less than commercial customers, acquisition policies should reflect the full cost of meeting these requirements and compensate industry fairly for delivering secure, compliant, and mission-ready solutions.

Incentivize technological superiority and lifecycle return on investment. Procurement strategies should emphasize best value over lowest price technically acceptable (LPTA) evaluations for better returns. For complex IT solutions, the lowest upfront price rarely delivers the lowest total cost or the strongest mission performance. Acquisition decisions should consider total cost of ownership, including integration, cybersecurity, and long-term sustainment. Rewarding industry partners that deliver measurable mission improvements and lifecycle savings encourages innovation while protecting taxpayer investment.
Policymakers should also recognize that ongoing technical and help desk support are integral to mission assurance. These lifecycle services ensure systems remain secure, compliant, and fully operational long after initial deployment.

Reinforce small and diverse business participation. Small businesses are critical to continual advancement, agility, and resilience in the federal IT marketplace. Policies that empower distributors and integrators to support small and disadvantaged firms help expand participation, maximize alternative IT solutions, and grow the nation’s technology workforce.

Conclusion

The federal IT ecosystem delivers far more than commercial off-the-shelf products. It is a vital national capability that fuels advancement, protects supply chain integrity, and ensures every agency can operate securely, efficiently, and effectively. Original Equipment Manufacturers drive progress through technology innovation. Distributors secure the supply chain, extend reach, and enable broad and diverse market participation. Information Technology Value-Added Resellers (ITVARs) tailor solutions to agency needs and bring the diversity, agility, and customer focus that strengthen competition. Systems integrators deliver and sustain the mission-critical platforms that power defense, intelligence, and civilian operations every day.

Treating IT as a commodity ignores this reality. It diminishes the benefit of the very partners that make government modernization possible. It also risks narrowing choice, slowing technological progress, and weakening the industrial base that supports national security. While visibility into agency spending is important, it should not come at the expense of flexibility or the ability to deliver mission outcomes. Efficiency and resilience are not opposing goals; both are essential.

The path forward is clear. Policymakers should strengthen, not shrink, the supply chain that empowers government to innovate. By focusing on best outcomes, open standards, and fair recognition of the unique requirements industry fulfills, government can achieve true savings and sustainable returns measured not only in dollars, but in security, readiness, and mission success.

Reconciling commercial classification with government-unique operational realities is essential for acquisition policy to achieve both fiscal responsibility and mission readiness.