COUNSEL COMMENTARY

SBIR Phase III Eligibility Clarified

A recent GAO decision provides guidance on when agencies may issue sole-source awards under the SBIR program.

BY STEPHEN L. BACON

The Small Business Innovation Research (SBIR) program is designed to fuel innovation while providing small businesses a pathway to federal contracts. The program also seeks to promote the commercialization of SBIR-derived technologies.

These objectives are advanced through a special acquisition preference that is afforded to SBIR program participants when agencies make "Phase III awards." The SBIR program's authorizing statute defines "Phase III" to include any "work that derives from, extends, or completes efforts by the SBIR participant in Phases I and II of the program."

The law provides that, "[t]o the greatest extent practicable," agencies "shall...issue, without further justification, Phase III awards relating to technology, including sole source awards, to the SBIR...award recipients that developed the technology."[1] This statutory Phase III preference gives agencies a streamlined method to procure SBIR-derived technologies.

In the protest of Digital Force Technologies, Inc., the Government Accountability Office (GAO) clarified the circumstances under which an agency may invoke its authority to award sole-source Phase III contracts.[2] GAO's decision gives agencies, SBIR participants, and protesters important guidance on when and how this unique contracting preference may be used.

Background

This protest involved the U.S. Air Force's requirement for a tactical security system (TSS), which was described as a "modular, scalable, tailorable, lightweight, rapidly deployable, ground-based security and surveillance system."[3] The Air Force plans to use the TSS to assist with protecting personnel and assets at remote deployment locations.

After conducting market research, the Air Force decided to fulfill this requirement using a Phase III award to either Clear Align or Anduril Industries, effectively excluding Digital Force from competing for an award.

After its agency-level protest was denied, Digital Force filed a subsequent protest at GAO to challenge the SBIR Phase III solicitations issued to Clear Align and Anduril. In response to that protest, the Air Force took corrective action and canceled those solicitations.

Instead, the Air Force decided to pursue a single Phase III solicitation issued only to Clear Align. The Air

Force's decision was premised on its determination that "Clear Align's proposed solution derives from, extends, and completes work from two prior SBIR phase II awards."[4]

Digital Force challenged the Air Force's decision on several grounds. GAO rejected all the arguments raised by Digital Force and, in doing so, GAO provided three key takeaways for government contractors to understand about Phase III awards.

The *Work* Must Derive From Prior SBIR Efforts

Digital Force argued that the Air Force's requirement for a tactical security system did not derive from Clear Align's prior SBIR work. According to Digital Force, the procurement did not qualify for Phase III treatment because the Air Force developed its requirements separately from any of Clear Align's previous SBIR contracts.

GAO disagreed, finding that Digital Force misconstrued the statute. The statute focuses on work that derives from prior SBIR efforts, not requirements that derive from those efforts.

As GAO explained, "the statute and the policy directive each expressly use the word 'work' when explaining SBIR phase III; they do not mention the agency's requirement."[5] Simply put, a proper SBIR phase III award must be for *work* that derives from, extends, or completes a prior SBIR effort.

The Air Force was able to satisfy that requirement by showing that Clear Align's proposed TSS solution derived from work completed on two prior SBIR contracts. To document this determination, the Air Force prepared a Determination and Finding (D&F) to "memorialize the agency's consideration of the relevant SBIR phase II efforts and explained their relevance to the instant procurement."[6]

Specifically, the Air Force concluded that Clear Align's proposed TSS included a camera that had been developed, in part, under prior SBIR contracts. Indeed, Clear Align's proposal explained that "key design concepts from the prior SBIR efforts have been refined and are embedded into its current generation of cameras."[7]

Moreover, the D&F included copies of the prior SBIR contracts that contained details of the work completed. This was sufficient to establish a connection between the prior SBIR contracts and Clear Align's proposed TSS solution.

COUNSEL COMMENTARY CONT'D

Key Takeaway: A contractor's eligibility for a Phase III award does not depend on how the agency writes its requirements. Rather, the agency must reasonably determine that the contractor's proposed solution builds upon its prior research and development efforts under the SBIR program.

Agencies should prepare comprehensive determinations and findings that clearly trace the connection between current work and prior SBIR efforts. Contractors pursuing Phase III opportunities should proactively provide detailed explanations of how their proposed solutions build upon previous research to support the agency's use of an SBIR Phase III award.

For competitors considering protests, *Digital Force* demonstrates the high bar for challenging Phase III awards. If the agency's Phase III determination is adequately documented, technical disagreements about connections between SBIR phases are unlikely to succeed.

SBIR-Derived Products May Be Only a Component of the System Procured

Digital Force complained that Clear Align's proposed TSS was made up of many commercial-off-the shelf (COTS) products and only a single component, the camera, could qualify as SBIR Phase III work. Digital Force contended that the SBIR statute did not authorize agencies to procure a collection of COTS items that were unrelated to Clear Align's prior SBIR efforts.

According to Digital Force, the Air Force's interpretation of the SBIR statute would lead to absurd results. Specifically, Digital Force argued that "a large defense contractor could purchase the rights to Clear Align's Z 320 MWIR camera, install the camera on a C-40 aircraft, and win an SBIR phase III award for the Air Force's C-40 fleet expansion program."[8]

GAO rejected Digital Force's hypothetical scenario. Unlike the "cautionary tale involving the Air Force's C-40 fleet expansion," Clear Align's "SBIR-derived component" – the Z 320 MWIR camera – "is reasonably related to the overall objective of the system the agency seeks to procure."[9] GAO noted, for example, that the required TSS needed "surveillance capability, motion detection, video assessment, and sensing technologies, and Clear Align is providing within its overall system, an SBIR-derived camera."[10]

Key Takeaway: Companies with SBIR-derived technology can potentially leverage Phase III authority for larger systems that incorporate their innovations, provided the SBIR component serves a meaningful role in the overall solution. Future cases are likely to test how close of a nexus is required between the SBIR-derived technology and the objective of the system procured by the agency.

Document Status as a Successor-in-Interest Entity

Digital Force also challenged whether Clear Align qualified as a "successor-in-interest" to Computer Optics, the company that performed the original SBIR Phase II work. This argument highlights a common complication in the SBIR ecosystem: small companies frequently merge, acquire assets, or undergo corporate changes between Phase II completion and Phase III opportunities.

The SBIR/STTR Policy Directive allows Phase III awards to entities that are successors-in-interest to the original SBIR participants. But what constitutes sufficient evidence of succession to qualify for a Phase III award?

In this case, Clear Align acquired the assets of Computer Optics through a detailed purchase agreement that transferred "all intellectual property used or usable in connection with the business, including, without limitation, patents, computer software and

data, trademarks, trade styles, trade secrets, know-how, processes, formulae, designs, drawings, [and] technical data."[11]

GAO found this sufficient to demonstrate that Clear Align qualified as a "successor-in-interest." The agency had reasonably concluded that Clear Align acquired the relevant intellectual property and could legitimately claim successor status.

> ***Key Takeaway:*** Companies acquiring or merging with SBIR participants should document transactions thoroughly. The asset purchase agreement should explicitly address intellectual property transfers, including SBIR-derived technology. This is critical to ensure that the resulting entity is eligible for Phase III awards as a "successor-in-interest" to the acquired entity.

Looking Forward

The *Digital Force* decision provides valuable clarity for the government contracting community. SBIR Phase III authority remains a powerful tool for agencies seeking to leverage successful research investments, even when that research represents only part of a larger system solution.

For SBIR companies, the decision confirms that Phase III opportunities can extend beyond narrow technical applications to broader system integrations. Success requires clear documentation of the connection between past research and current proposals, along with proper handling of any corporate succession issues.

For competitors considering protests, *Digital Force* demonstrates the high bar for challenging Phase III awards. If the agency's Phase III determination is adequately documented, technical disagreements about connections between SBIR phases are unlikely to succeed. Challenges should focus instead on clear procedural violations or obvious misapplications of Phase III authority.

Most importantly, the decision underscores that SBIR Phase III procurement operates under different rules than traditional competitive acquisitions. Understanding these distinctions and planning accordingly remains essential for success in this unique corner of the federal marketplace. **CM**

Stephen L. Bacon is a shareholder in the Washington, D.C. office of the law firm Rogers Joseph O'Donnell, where he represents government contractors in bid protests, claims, terminations, investigations, and suspension and debarment proceedings. He frequently litigates cases at the Court of Federal Claims, the Government Accountability Office, the Boards of Contract Appeals, and the Small Business Administration's Office of Hearings and Appeals. He also provides advice and counsel to clients on a broad range of contractual and regulatory compliance issues that confront government contractors.

The views expressed in this article are those of the author and do not necessarily reflect the views of Rogers Joseph O'Donnell or its clients. This article is for general information purposes and is not intended to be and should not be construed as legal advice.

ENDNOTES

1 15 U.S.C. § 638(r)(4).
2 Digital Force Technologies, Inc., B-423319, May 19, 2025, 2025 CPD ¶ 114.
3 Id. at 2.
4 Id. at 4.
5 Id at 7 (citing 15 U.S.C. § 638(e)(4)(C); SBIR/STTR Policy Directive (May 2023) § 4(c).
6 Id. at 13.
7 Id. at 9.
8 Id. at 10.
9 Id. at 14.
10 Id.
11 Id. at 16.

CMBOK™ COMPETENCIES B.5 1.7 3.3 4.2

Avoid the Cost of Counterfeits

It's impossible to eliminate all counterfeits, but there are many strategies and tools to identify them and minimize risk.

By Sarah Baire

My official start in supply chain began with Blockbuster in 2007. As part of the on-the-job training, we were taught to identify fake bills that could be used by counterfeiters during cash transactions.

Although we had access to counterfeit ink pens, there were times when the ink dried out, or we were waiting for a delivery of new pens to arrive, and we would need to utilize other visual eye techniques to verify that bills were not counterfeit during cash transactions.

If a counterfeit bill was missed by the store, then it was caught by the bank during the morning deposit, and it would lead to disciplinary action against the store manager and employees for lack of due diligence during cash transactions.

Fast forward to today, and I hardly carry cash anymore. When I use cash, I cannot remember where I spend it as much as I do when I use my debit card for transactions. However, if I do pull cash to use, or whenever I receive cash back from transactions, my first instinct is to examine the cash received to ensure that counterfeit dollars are not being given back to me, as I don't want to carry that risk, thanks to my training from Blockbuster. This early exposure to counterfeit risk sharpened my awareness about authenticity.

Authenticity, once a lesson from a cash drawer, now feels like an ingrained reflex that translates beyond cash, where I find myself questioning the legitimacy of every transaction – personally and professionally. I ask myself, "Is this product genuine? Can I trust the source this product came from?"

Counterfeit money is not a new concept, nor is it the only commodity that is being fabricated by counterfeiters. In today's global supply chains, counterfeits include shoes, airbags, semiconductors, software, medication, personal protective equipment, and more.

A counterfeit good is an imitation of a genuine product that is created without the consent of the manufacturer and can be of substantially lower quality than the authentic product. It is often poorly made due to the lack of quality or environmental controls by using dangerous or toxic chemicals and materials.[1]

- Have you ever bought one of those event t-shirts that get sold outside of the venue for a cheaper price only to find the glaringly obvious typos afterwards, or see that the print fades after the first wash?
- Have you ever bought that name-brand bag or shoe that was really a "knock off," but no one could tell unless they looked at the tag?
- Have you ever been swindled by resale venue tickets?
- Have you ever ordered from a "too good to be true" e-commerce website?

If you said yes or nodded/smiled to any of the above situations because you or someone you know went through it, then you are not alone. We are taught to find the best value for our dollar, and sometimes that means we compromise quality and source of supply over price.

As a supply chain professional, headlines such as those shown in Figure 1 give me pause, and I ask, "Which part was the contributing factor to the defect? Would a root cause analysis show that the part was counterfeit?"

The Problem

Supply chains in all industries are at risk of a counterfeit part entering their markets, which can disrupt and create devastating impacts – either financially or reputationally. In some instances, there may be no chance of bouncing back from that one-time mistake.

Beyond customer frustration, counterfeit goods pose serious operational and safety risks – particularly when they infiltrate regulated industries like aerospace, defense, or health care.

According to the U.S. Immigration and Customs Enforcement (ICE) website, "Some of the most dangerous counterfeit

FIGURE 1. Counterfeits in the News

products involve automotive parts, electronics, safety equipment, prescription drugs, and cosmetics due to the potential threats they present to public safety and public health."[2]

Supply and Demand Equals Opportunity

Business 101 teaches us that the price of a good or service will fluctuate depending on supply and demand. That same fluctuation creates an opportunity for counterfeit parts to enter the market. According to a report published by the National Association of Manufacturers, "counterfeiters have gained strength due to the growth of e-commerce platforms, which have transformed how companies connect with customers and changed the marketplace for selling goods."[3]

These trends reveal how even sophisticated teams can be fooled, especially when under pressure to fill gaps quickly. According to the Government Accountability Office (GAO), counterfeiters will post pictures of the authentic goods on the e-commerce website, then fill those orders with fakes.[4]

In 2018, GAO reported that it purchased 47 assorted items from third-party retailers using e-commerce websites, and of those 47 items purchased, 20 were found to be counterfeit, which included products such as makeup and electronics.[4]

Organizations should use their procurement team to vet e-commerce websites that are selected as the potential source of supplies before placing orders to reduce the risk of receiving counterfeit parts.

Force Majeure

A force majeure is when an unforeseeable event occurs that is out of the supplier's control, including events such as war, natural disasters (tornadoes, hurricanes, floods, tsunamis, fires, blizzards, etc.), and pandemics. Depending on the severity of the disaster, it can create conditions that allow counterfeit parts to enter the market.

During the COVID-19 pandemic, the world consumed many 3M N95 masks as personal protective equipment (PPE) to reduce the transmission of the SARS-CoV-2 virus. In 2021, counterfeit N95 masks were found to be sold in at least five states to various hospitals, medical facilities, and government agencies that led to a federal investigation.

Counterfeiters took advantage of the COVID-19 pandemic by preying on the consumer's increased anxiety and fear during social distancing measures.[3] Rather than going out in public to purchase goods, consumers' fear created an increase in e-commerce purchases. When panic and urgency meet limited oversight, counterfeiters seize the moment.

Impacts of Counterfeit Parts

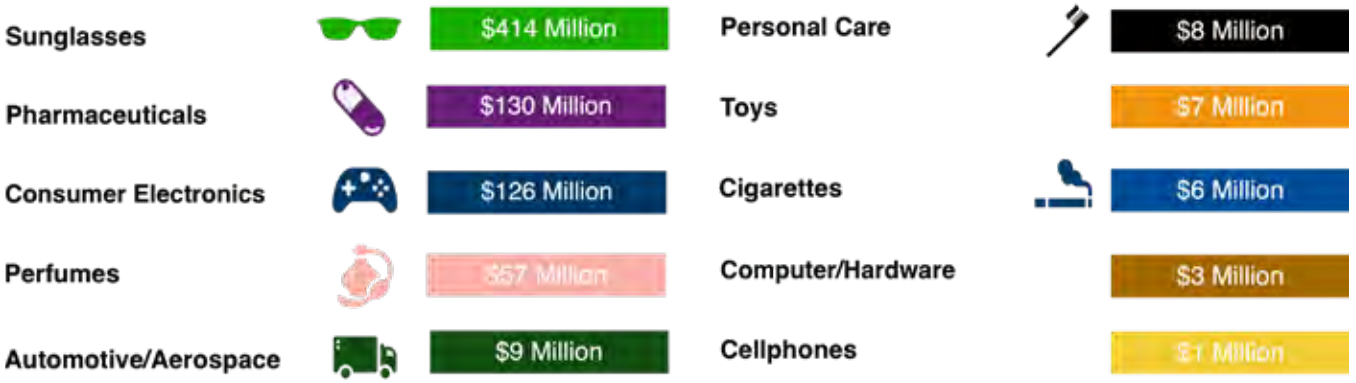
According to the U.S. Customs and Border Protection (CBP) website, "counterfeit goods are often low quality and pose threats to consumer safety, security, and health – it is imperative that consumers purchase from reputable sellers to avoid these harmful risks."[5]

Federal agencies have already documented the widespread impact of counterfeit goods. In 2023, CBP seized various counterfeit products that could have been hazardous to the safety of American citizens (see Figure 2).

The CBP has reported that "e-commerce is altering global trade by allowing for more cross-border transactions and by giving counterfeiters direct access to consumers."[4]

In February 2020, the U.S. Library of Congress released a report entitled, "U.S. Intellectual Property and Counterfeit

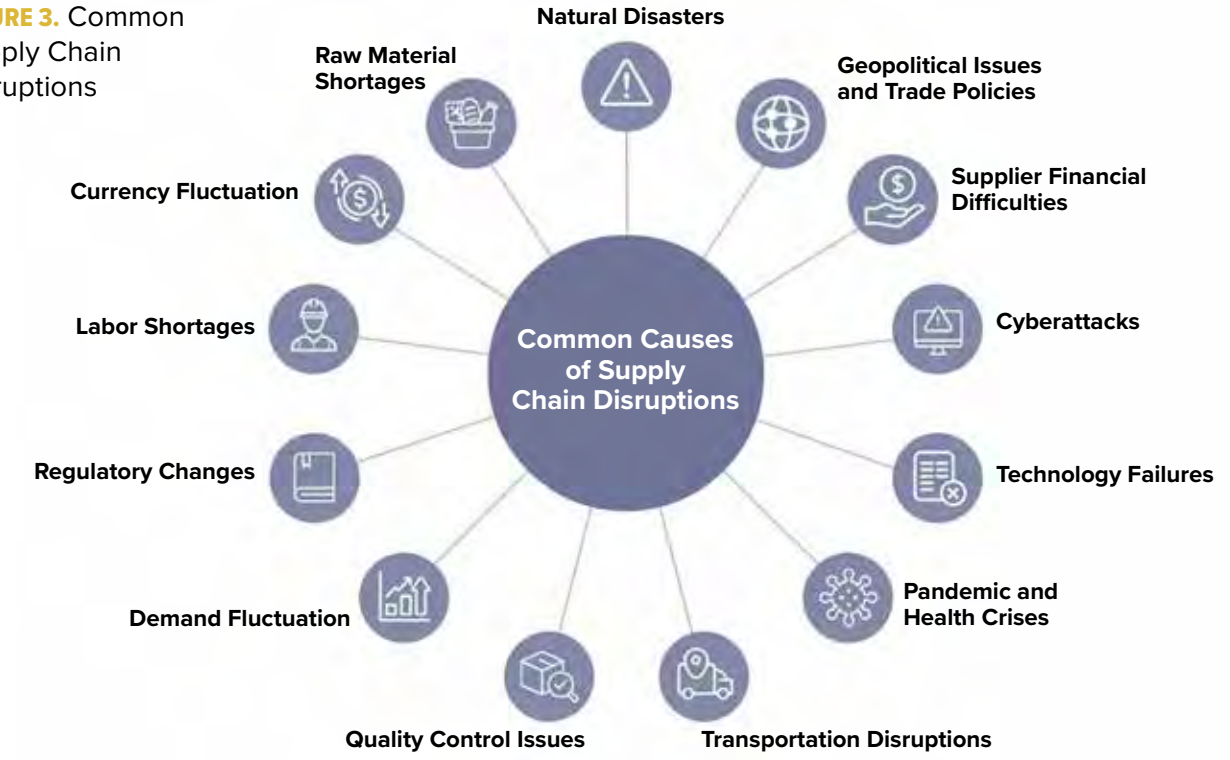
FIGURE 2. Most Seized CBP Counterfeit Commodities of FY24



Total Quantity of Health, Safety, and Security Seizures: 7,002,899
MSRP Value of Health, Safety and Security Seizures: $761,293,233

Source: Adapted from www.cbp.gov/trade/fakegoodsrealdangers

FIGURE 3. Common Supply Chain Disruptions



Goods – Landscape Review of Existing/Emerging Research." The report noted, "as of 2018, counterfeiting is the largest criminal enterprise in the world, with domestic and international sales of counterfeit and pirated goods totaling between an estimated $1.7 trillion and $4.5 trillion a year."[6]

During the COVID-19 pandemic in 2020, counterfeiters were given an opportunity to profit even more with the dramatic disruptions within the supply chain after many countries shut down their production and shipping lines. This large-scale shutdown created a massive bullwhip effect in balancing supply and demand.

Supply Chain Disruptions

Accurate supply chain forecasting is not always easy for organizations to maintain because risk factors occur that will disrupt and change the way an organization's supply chain operates. Any disruption in the supply chain is an opportunity for a counterfeiter to enter the market with a good or service that was impacted by that disruption.

To better understand where counterfeits can slip in, it is important to examine the common causes of supply chain disruptions as shown in Figure 3.[7]

These supply chain disruptions can lead to financial, operational, and reputational impacts.

- *Financial* – According to the Department of Homeland Security (DHS), "The growth in online sales of counterfeit and pirated goods directly harms – and unfairly competes against – the many legitimate companies that produce, sell and distribute genuine goods, often resulting in lost profits, employee layoffs, and diminished incentives to innovate."[8]
- *Operational* – Labor shortages, material shortages, natural disasters, and technology failures can lead to various operational impacts. These disruptions can lead to production shutdowns, which costs organizations time and money. Material shortages are the largest contributor to production shutdowns. When material shortages occur, an organization may try to use e-commerce websites to find alternative sources of supply for its parts. Counterfeiters have learned to remove the typical red flags that buyers may use to distinguish a genuine product from a fake product, including pricing discrepancies, online reviews, or language used to describe the product.[3]
- *Reputational* – Quality plays a key role in an organization's reputation. If an organization does not have the

right processes in place to identify counterfeit parts upon delivery and inspection, then that purchase may lead to potential quality failures. Quality control failures can lead to defects, product recalls, accidents, injuries, and/or loss of life that can result in lawsuits, fines, regulatory penalties, and loss of reputation. In 2013, Takata Corporation had to issue a recall of 67 million airbags due to airbag inflators exploding and releasing metal shards throughout the passenger cabin of the vehicle when exposed to extreme heat. These explosions led to 27 deaths and more than 400 injuries. The Takata Airbags Recall cost the company billions of dollars in damages, which led to the company filing for bankruptcy in 2017. The recall also damaged the reputation of the automakers who used the Takata Airbags in their vehicles, even though Takata was the original equipment manufacturer (OEM) of the product.

Regardless of the cause of the supply chain disruption, counterfeiters will exploit it to their advantage, which is why it is crucial for organizations to place emphasis on vetting and using the correct sources of supply for their procurements.

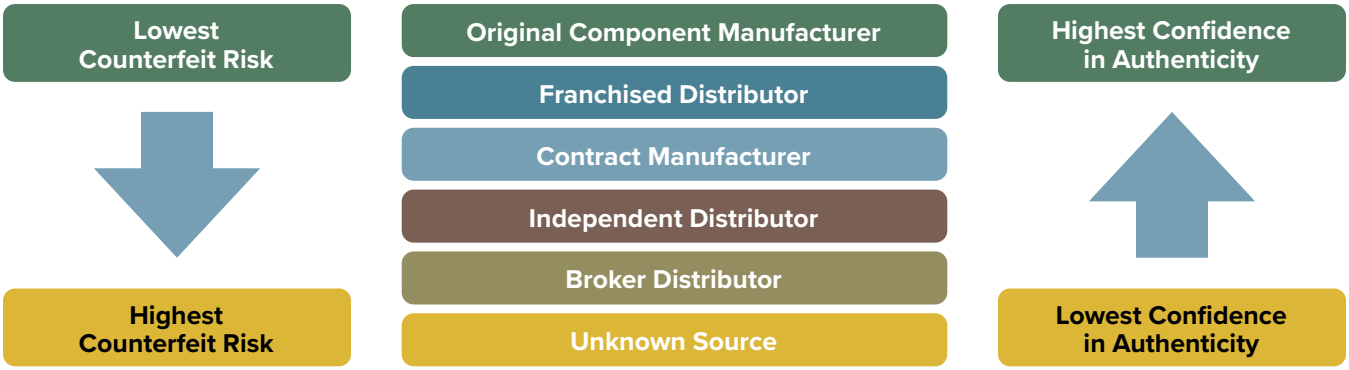
NASA provides an illustration in its Counterfeit Parts Awareness and Inspection training course to show the importance of an organization's source of supply for its material (see Figure 4). On the left, we see the lowest counterfeit risk being an organization purchasing from the original component manufacturer (OCM) or OEM and the highest counterfeit risk being an organization purchasing from an unknown source. On the right, we see that the highest confidence in authenticity also lies with the OCM/OEM, whereas the lowest confidence in authenticity is purchasing from an unknown source.[9]

Seven Main Types of Counterfeits

Counterfeit goods can be categorized into seven main types: Recycled, Remarked, Overproduced, Out-of-Spec/Defective, Cloned, Forged Documentation, and Tampered.[10]

- *Recycled* – When individual parts are removed from used systems to be repackaged and sold in the market as new individual parts. *Example:* In 2016, after the Takata Airbag recall, Hyundai launched a campaign to educate Americans about the dangers of counterfeit auto parts. Hyundai advised that some shops would recycle crash parts as "new" for customers seeking part replacements.[11]
- *Remarked* – When original markings on a part are removed and remarked with false information. *Example:* In 2023, numerous airlines were grounded due to counterfeit bolt and bracket parts being used on the aircraft, which, on one flight, caused the tail section of the turboprop to tear loose. Counterfeiters will brand MIL-spec part numbers onto counterfeit-made MIL-type connectors.[12]
- *Overproduced* – When unauthorized agents have access to an organization's intellectual property, they could manufacture goods outside the organization's contract to sell excess inventory on the open market. *Example:* In the automotive industry, there is a higher degree of wear and tear that leads to the constant demand and overproduction of replacement parts. The most counterfeited automotive parts are brake pads, bearings, drive belts, oil filters, piston rings, spark plugs, steering parts, and valves. Consumers are misled by the size of the part versus the lower cost and do not realize the quality impact that the counterfeit part may have on the performance of their vehicle.[13]

FIGURE 4. Source of Supply – Counterfeit Risk and Confidence in Authenticity



- *Out-of-Spec/Defective* – An unauthorized agent may use the organization's intellectual property to knowingly sell defective and out-of-spec parts on the open market. *Example:* Since the COVID-19 pandemic, there has been a rise in counterfeit drugs and pharmaceuticals. According to the World Health Organization (WHO), counterfeiters sell products authorized for sale on the open market; however, these products fail to meet quality standards and/or specifications, such as improper storage or expiration.[14]
- *Cloned* – This refers to parts that are copied using reverse engineering or by obtaining an organization's intellectual property illegally. *Example:* Reverse engineering has been known to occur with Nike brand shoes manufactured in China. A product design subject matter expert will buy an authentic pair of Nike shoes, deconstruct it, then draw up a design for production to create the counterfeit version that is sold into the supply chain as authentic.[15]
- *Forged Documentation* – Documentation that provides a false certification of compliance standards for that part (e.g., serial numbers, lot/date codes, expiration dates, material, ingredients, etc.) *Example:* According to the United States Patent and Trademark Office (USPTO), some counterfeiters use fake certification marks on their products to indicate that the product meets certain quality and safety requirements. USPTO advises comparing the packaging artwork of the suspect part against the packaging artwork of the known authentic good.[16]
- *Tampered* – Synonymous with a "Trojan horse," tampered parts can occur at the software/firmware level and can function as a backdoor for the counterfeiter when the part is implemented into a system. *Example:* Like the cloned example above, counterfeiters will purchase authentic hardware, then modify and replace it with malware to redistribute that part back into the supply chain with the goal of targeting and disrupting organizational information technology environments that perform critical functions.[17]

Even with training and vigilance, the most seasoned supply chain professionals can struggle to spot a real product versus a counterfeit product.

Counterfeit Risk Avoidance

What is counterfeit risk avoidance? Counterfeit risk avoidance involves an organization taking proactive measures to implement policies and procedures that

FIGURE 5. Can you spot the counterfeit good?*

* ANSWERS LISTED IN THE BOTTOM RIGHT CORNER ON PAGE 25

combat counterfeit parts from entering its supply chain by establishing robust quality control plans and using reliable sources of supply for procurements.

Counterfeit products can never be entirely eliminated from the supply chain; however, if an organization implements the proper safeguards, then the counterfeit risks listed earlier can be significantly reduced. The three steps outlined below demonstrate how to do this.

1. Value of Processes/Procedures

An organization should take particular care in creating its policies and procedures. Well-written policies and procedures help ensure compliance and accountability, maintain consistency and efficiency, and create opportunities for continuous improvement that drive higher productivity and better quality of service.

Internal Work Instructions

An organization's work instructions provide the framework for how the supply chain is supposed to function, including procurement instructions, supplier expectations, and quality and receiving requirements. If the work instructions are vague, it leaves room for interpretation by the person reading them, which may lead to future risks.

The internal work instructions should be communicated clearly and concisely to the reader to ensure they understand the message and the organization's expectations. If expectations are unclear, it is unreasonable to expect suppliers to interpret or enforce those instructions correctly.

Procurement Engagement Now, Not Later

No one knows the organization's source of supply better than the procurement department. The best way to ensure that all contract requirements are met is to reach out to procurement first to find the best source of supply that has already been vetted and added by the organization.

If a new supplier needs to be added to the organization's source of supply, then there needs to be a strict onboarding process that vets the supplier to ensure that there will not be a potential operational or financial risk to the organization.

2. Value of Vetting Suppliers Before Onboarding

Organizations need to ensure that they conduct due diligence when onboarding new suppliers by having the supplier undergo a thorough vetting process. An organization should complete the following (at a minimum) before adding a new supplier to its source of supply:

- Conduct background checks.
- Check supplier references.
- Evaluate the supplier's financial stability.
- Review the supplier's quality certifications and processes.
- Assess the supplier's technological capabilities.
- Conduct site audits to ensure that the supplier is following industry standards and regulations, labor laws, and environmental standards.
- Confirm the supplier's production capacity and capabilities.

If a supplier does not meet all the necessary criteria for the organization, then they should not be added as a source of supply.

Communicating Expectations

The perfect time to communicate the organization's supplier performance expectations is during the onboarding process. When an organization fails to clearly relay those expectations to the supplier, then how can it expect them to succeed?

Not every organization operates the same way, so it can never be assumed that one size fits all for performance metric criteria as a supplier. An organization that emphasizes supplier performance metrics and provides training during the onboarding process will help mitigate future financial, operational, and reputational risk impacts.

Supplier Site Visits – Do They Walk the Talk?

Any supplier can "talk a good game." However, that is why it is important that the organization conducts a site visit during the onboarding process to ensure that the supplier is walking the talk with their processes and procedures.

As noted above, forged documentation is a common counterfeit type, which means that a supplier could provide forged documentation to show that they hold quality certifications and not actually adhere to the quality processes under that certification. A site visit would confirm that the supplier is following the processes of those quality certifications.

Training

As mentioned previously, organizations should provide new suppliers with adequate training during their onboarding processes regarding the organization's expectations for processes and procedures. Suppliers cannot be expected to succeed on day one with a new customer, especially if that customer has vastly different processes than their other customers.

If an organization provides training and resources to answer frequently asked questions, along with a company ambassador that a supplier could reach out to for follow-up questions, then it will help create a more collaborative relationship

for both parties to ensure that quality expectations are met.

3. Value of Quality

The three main criteria a professional considers when making a purchase are delivery schedule, price, and quality. The running joke in procurement is "pick two," since obtaining all three would be considered the "perfect procurement," which can be challenging in today's supply chain environment.

In those "pick two" situations, we rarely see someone choose the supplier that does not fit the quality option. This section provides quality suggestions to help ensure your procurement team is sourcing the right source of supply for the organization's needs.

Quality Note Requirements

Part deliverables should be defined by their quality note requirements. Part complexity and applicability will determine which quality notes would be used, and customer contract requirements will also provide an organization direction on what is needed to be compliant with their contract deliverables.

However, if the organization does not flow clearly defined requirements into their quality notes, then the organization may not receive the information that it needs, especially if/when failures arise, and we must answer "why" to leadership.

Case Example: When OEM Requirements Are Missed

A standard scenario involves a quality note requesting that a supplier provide a Certificate of Conformance/Compliance (CofC) upon delivery of the material. If the quality note does not specify that the supplier needs to provide an OEM CofC, then the supplier will not be required to provide one contractually. If one is needed after delivery, then the supplier may request a fee to provide the OEM CofC because the request was not clearly defined. What happens if the supplier cannot provide an OEM CofC and the purchase order is non-cancellable, non-returnable (NCNR)? Typically, the organization will eat the cost through the loss of profit on that purchase by purchasing the part again using the correct quality note requirements to ensure compliance. This scenario not only creates a new purchase order, which involves more dollars being spent on material, but it involves numerous supply chain folks, such as program management, procurement, quality, production control, shipping/receiving, and finance to remedy the situation, which adds unanticipated labor costs for an order that was only needing an OEM CofC.

Quality Control Systems

According to Embry-Riddle Aeronautical University Scholarly Commons, "Effective quality control systems are critical in aircraft maintenance because they reduce the need for rework, which in turn shortens turnaround times and lowers overall maintenance costs."[18]

The quality note requirements help define the quality control system the supplier needs to have to deliver that part for the organization. For example, suppliers that obtain ISO 9001, ISO 14001, and/or AS9100 quality certifications should be valued over suppliers that may not hold these quality certifications.

Suppliers that obtain these types of certifications are committed to the idea of continuous improvement. These suppliers will establish processes and procedures that implement industry standards and regulatory requirements, along with customer requirements, to deliver high-quality products or services. The quality note for the part could mandate that procurement be required to go to a source of supply that has one of these valid quality certifications.

Supplier Documentation

Quality note requirements will also dictate the required documentation that must be provided by the supplier. These include:

- A Certificate of Conformance (CofC)
- An Original Equipment Manufacturer CofC that includes serial numbers, lot/date codes, and/or expiration date information
- A test analysis or Certificate of Analysis (CofA)
- A first article inspection, or source inspection
- NADCAP certifications
- Counterfeit compliance/avoidance requirements

Determining what supplier documentation is required prior to order placement will help procurement determine the source of supply for that part. However, it is important to note that organizations also need to confirm that the supplier documentation matches the parts that were provided. This practice should be a part of the receiving inspection process to ensure that suspect parts do not enter the organization's supply chain.

Physical Inspections

Using the right source of supply never guarantees that organizations will eliminate counterfeit parts from entering their supply chain; however, the next safeguard is to ensure that an organization's supply chain mitigates counterfeit risk by incorporating a physical inspection process at the time of material delivery.

Answers to Figure 5:
The counterfeit items are **A, D, F, G**

FIGURE 6. The Do's and Don'ts to Mitigate the Risks of Counterfeits

DO

- Engage procurement early to identify approved, trustworthy sources of supply to prevent last-minute shortcuts.
- Vet new suppliers thoroughly before onboarding by reviewing certifications, conducting site visits, and checking references to ensure reliability and compliance standards for your organization.
- Train suppliers during onboarding to set clear expectations and reduce miscommunication.
- Use well-defined quality note requirements on all procurements to ensure suppliers meet your contractual and technical standards.
- Incorporate physical inspections training into receiving processes to catch suspect parts before they enter your system.
- Report suspected counterfeit parts via sources like GIDEP to help eliminate them from all supply chains, not just your organization's supply chain.

DON'T

- Assume all suppliers are equal. Lack of due diligence during the onboarding process creates a long-term risk for an organization.
- Delay involving procurement. Waiting until the last minute can lead to rushed purchases from unverified sources of supply, which increases the risk of counterfeit.
- Rely solely on supplier-only documentation. Certificates need to be verified for authenticity against the parts through visual eye checks and part testing.
- Create vague receiving processes and procedures for your organization's parts. Unclear instructions and expectations increase the chance of quality failures and compliance issues.
- Ignore pricing "red flags." If it seems too good to be true, then it probably is.
- Send suspect counterfeit parts back to the supplier, as this allows counterfeit items to reenter circulation in other organization's supply chains.

Physical inspections before official part acceptance from the supplier will help ensure that suspect parts are identified and removed before being released into the organization's supply chain. If a suspect part is found, then the recommendation is to report the part – do not send it back to the supplier - as the goal is to eliminate the counterfeit part from entering the supply chain altogether, not just the supply chain for one organization.

Available Resources

The resources below primarily refer to counterfeit electronic parts versus other commodities; however, the general concepts in these resources can be applied to how an organization sources its supply of goods and services. The consensus from these resources is that selecting the right source of supply is the best way to mitigate the risk of purchasing counterfeit products.

Defense Federal Acquisition Regulation Supplement (DFARS)

Review the language in DFARS 252.246-7007 Contractor Counterfeit Electronic Part Detection and Avoidance System.[19]

Society of Automotive Engineers (SAE) International

Review the language in SAE Aerospace Standard AS6081 – Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors.[20]

GIDEP

In DFARS 252.246-7007, the language references the Government-Industry Data Exchange Program (GIDEP). GIDEP "is a cooperative activity between government and industry participants seeking to reduce or eliminate expenditures of resources by sharing technical information essential during research, design, development, production, and operational phases of the life cycle of systems, facilities, and equipment."[21]

U.S. Department of Commerce

According to the U.S. Department of Commerce website, the best way to ensure that you are "getting the real thing" is to look for the four P's:[22]

- *Place* – Double check the source of supply.
- *Price* – If it looks too good to be true, then it probably is and should be checked against other sources of supply for packaging and product similarities.
- *Packaging* – Check the packaging for misspellings, blurred details, and graphic color imbalances.
- *Product* – Does the product look exactly like what was purchased before? Compare the labels.

While it is impossible to completely eliminate counterfeit parts from an organization's supply chain, ensuring that sources of supply are authentic, and incorporating proper safeguards during receiving inspection can significantly reduce the risk of purchasing counterfeit parts. CM

Sarah Baire has 15 years of supply chain experience in the aerospace and defense industry, with 12 years in procurement/subcontracts and three years in material management. She is the Vice President of the Florida Space Coast Chapter for the Association of Supply Chain Management (ASCM) and has spoken on the topic of counterfeit parts in aerospace and defense at the NCMA World Congress in 2024, the SIG 2024 Conference, and the ISM 2025 Conference.

ENDNOTES

1 "Counterfeiting (Intended for a Non-Legal Audience)." International Trademark Association, Archived November 14, 2024.

Accessed April 27, 2025. https://www.inta.org/fact-sheets/counterfeiting-intended-for-a-non-legal-audience/.
2 "Counterfeit Goods: A Danger to Public Safety." U.S. Immigration and Customs Enforcement (ICE), Archived June 3, 2025. Accessed July 02, 2025. https://www.ice.gov/features/dangers-counterfeit-items.
3 "Countering Counterfeits: The Real Threat of Fake Products." National Association of Manufacturers, Archived July 2020. Accessed April 25, 2025. https://www.nam.org/wp-content/uploads/2020/07/CounteringCounterfeits.vF_.pdf.
4 "Intellectual Property: CBP Has Taken Steps to Combat Counterfeit Goods in Small Packages but Could Streamline Enforcement." GAO-20-692, Archived September 2020. Accessed April 25, 2025. https://www.gao.gov/assets/gao-20-692.pdf.
5 "The Truth Behind Counterfeits." U.S. Customs and Border Protection, Archived June 9, 2025. Accessed July 02, 2025. https://www.cbp.gov/trade/fakegoodsrealdangers.
6 "U.S. intellectual Property and Counterfeit Goods: Landscape Review of Existing/Emerging Research." Library of Congress, U.S. Patent and Trademark Office, and U.S. Department of Commerce, Archived February 2020. Accessed April 25, 2025. https://www.uspto.gov/sites/default/files/documents/USPTO-Counterfeit.pdf.
7 Abby Jenkins, "Supply Chain Disruptions: An Expert Guide." Oracle NetSuite, Archived November 14, 2024. Accessed April 25, 2025. https://www.netsuite.com/portal/resource/articles/erp/supply-chain-disruptions.shtml.
8 "Combating Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States." U.S. Department of Homeland Security Office of Strategy, Policy and Plans, Archived January 24, 2020. Accessed April 25, 2025. https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf.
9 "NASA Counterfeit Parts Awareness and Inspection." Archived 2015. Accessed March 24, 2025. https://mttc.jpl.nasa.gov/pdf/NASA_Counterfeit_Training_unlimited_distribution_handout.pdf.
10 "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain." Proceedings of the IEEE, Archived August 2014. Accessed April 27, 2025. https://www.researchgate.net/publication/264124589_Counterfeit_Integrated_Circuits_A_Rising_Threat_in_the_Global_Semiconductor_Supply_Chain.
11 "Hyundai Launches Campaign to Educate Americans on the Danger of Counterfeit Auto Parts." Hyundai Newsroom, Archived February 10, 2016. Accessed July 01, 2025. https://www.hyundainews.com/en-us/releases/2126.
12 David Shaff, "Counterfeit Components Ground Airlines." Archived December 12, 2023. Accessed July 02, 2025. https://connectorsupplier.com/counterfeit-components-ground-airlines/.
13 "Automotive Fakes - Winning the Race Against Counterfeiters." Ennoventure. Accessed July 02, 2025. https://ennoventure.com/blogs/automotive-vehicle-fake-spare-parts-anti-counterfeiting/.
14 Kalliroi S. Ziavrou, Stephen Noguera, and Vassiliki A. Boumba, "Trends in Counterfeit Drugs and Pharmaceuticals Before and During COVID-19 Pandemic." Forensic Science International, Archived July 13, 2022. Accessed July 02, 2025. https://pmc.ncbi.nlm.nih.gov/articles/PMC9277998/.
15 "Tracing the Counterfeit Shoe Market." U.S. Immigration and Customs Enforcement (ICE), Archived February 10, 2022. Accessed July 02, 2025. https://www.ice.gov/factsheets/counterfeit-shoe-market.
16 "The Basics of Counterfeit Goods." U.S. Patent and Trademark Office. Accessed July 02, 2025.
17 https://www.uspto.gov/sites/default/files/documents/Basics%20of%20Counterfeit%20Goods.pdf
18 "Validating the Integrity of Computing Devices." NIST Special Publication 1800-34, Archived December 2022. Accessed July 02, 2025. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-34.pdf.
19 "Statistical Analysis to Evaluate the Impact of Quality Control and Quality Assurance on the Aircraft Maintenance Turnaround Time." Embry-Riddle Aeronautical University International Journal of Aviation, Aeronautics, and Aerospace, Volume 10, Issue 4, 2023. Accessed July 02, 2025. https://commons.erau.edu/cgi/viewcontent.cgi?article=1851&context=ijaaa.
20 "DFARS 252.246-7007 Contractor Counterfeit Electronic Part Detection and Avoidance System." Acquisition.gov, Updated January 17, 2025. Accessed April 25, 2025. https://www.acquisition.gov/dfars/252.246-7007-contractor-counterfeit-electronic-part-detection-and-avoidance-system.
21 "Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors AS6081." SAE International, Archived November 07, 2012. Accessed April 27, 2025. https://www.sae.org/standards/content/as6081/.
22 GIDEP. Accessed April 27, 2025. https://www.gidep.org/content/about-gidep.
23 "Shop Smart and Stay Safe This Season." U.S. Department of Commerce, Archived December 17, 2021. Accessed April 27, 2025. https://www.commerce.gov/news/blog/2021/12/shop-smart-and-stay-safe-season.

CMBOK™ COMPETENCIES B.1 1.1 1.4 C.1

Bridging a Gap in AI Contract Analysis

Augmenting AI with custom training/prompting can improve its ability to analyze local laws, industry regulations, and company policies.

By Niraj Ittan

Contracts govern the foundational agreements in business, setting clear expectations, responsibilities, and obligations. With the rise of artificial intelligence (AI), particularly large language models (LLMs), contract analysis has become significantly more efficient.[1]

As AI can now think and reason, AI-based contract review systems can assist with risk evaluation, contract analysis, and generating suggestions based on general contract principles. However, AI struggles to analyze jurisdiction-specific laws, company policies, or industry-specific regulations; here, generic AI models reach their limitations.

This article explores how AI can handle specific contract analysis, where it struggles with localized policies, and how an intelligent augmentation system can bridge this gap.

The Monkey Story: Learning Like AI

Before we discuss how AI struggles with local policies, it's important to understand the evolution of AI. Let's start by trying to understand different types of AI with an example.

Act 1: Traditional AI

Imagine a monkey being shown thousands of hand-drawn sketches of different fruits. Each time a sketch appears, the name of the fruit is spoken aloud – "apple," "banana," or "grape," for example.

Over time, the monkey learns to recognize the pattern and correctly identify the fruit by matching the visual image with the spoken word.

This is similar to traditional AI (also known as classical AI), which follows predefined rules or patterns learned from past data but cannot create anything new. It excels at classification and extraction tasks based on structured inputs.[2]

TABLE 1. AI Characteristics

TYPE OF AI	DETAILS	USE CASE
Traditional AI	Rule-based, structured data handling, predefined logic	Clause extraction tool; obligation tracker
Generative AI	Creates new content based on context, not just past data. It doesn't just follow rules – it can generate responses or draft documents based on context.	Contract summary generator; clause drafting assistant
Agentic AI	Refers to AI systems that can autonomously plan, make decisions, and take actions to achieve goals with minimal human intervention. An intelligent assistant that can execute multiple steps, not just respond to a single prompt.	AI contract reviewer; end-to-end contract assistant

Act 2: Generative AI

Now, imagine that the monkey learns to recognize fruits and understands how the sketches are drawn.

When asked, the monkey can create new sketches of fruits it has seen — or even invent sketches of imaginary fruits.

This represents generative AI: it learns patterns, but also generates new content such as summaries, emails, images, or legal clauses based on context, not just strict rules.[2]

Act 3: Agentic AI - A Step Beyond

Finally, picture the monkey recognizing and drawing fruits and planning a fruit basket display: choosing which fruits to pick, arranging them beautifully, and even inviting friends to admire them.

It can autonomously decide what to do next based on a goal, such as "make a fruit basket", without needing step-by-step instructions.

This illustrates agentic AI: an intelligent assistant that plans, makes decisions, and executes multiple steps toward achieving a goal with minimal human input.

Agentic AI represents the future of artificial intelligence – systems that go beyond answering prompts or generating content. They can autonomously reason, prioritize tasks, interact with humans and other systems, and adapt dynamically to changing goals.[3]

As technology advances, agentic AI will play a crucial role in transforming industries, including contract management, by handling complex,

multi-stage processes with limited human intervention. The differences across AI types are summarized in Table 1.

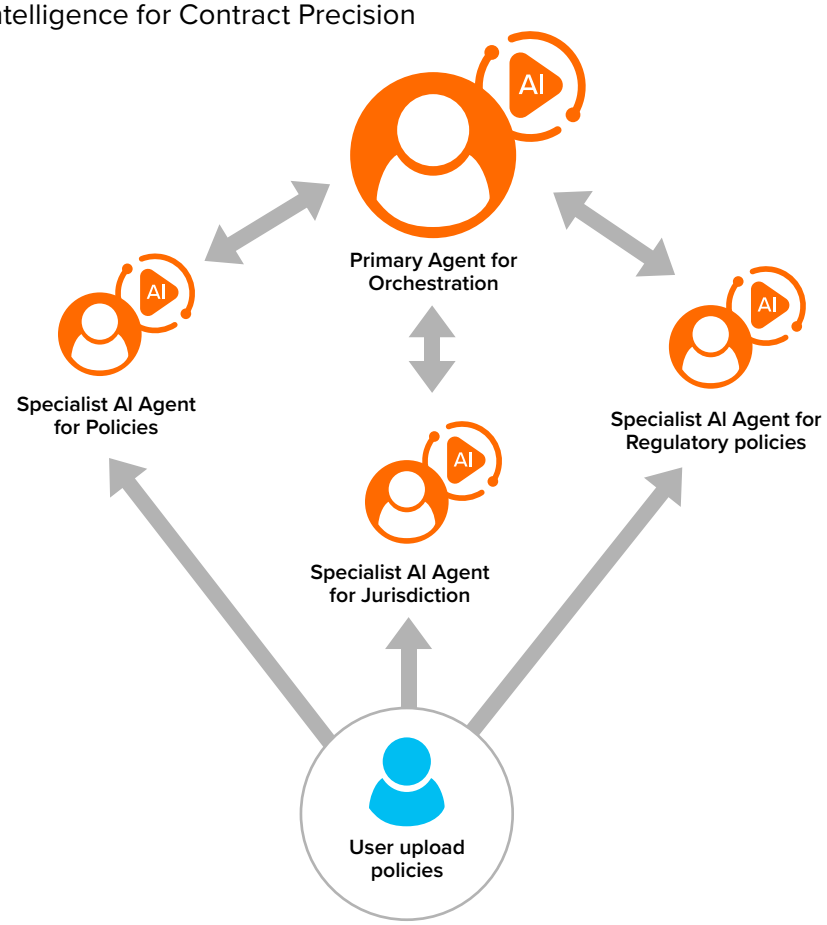
The Strength of Generic AI in Contract Analysis

Now that we understand the evolution of AI, let's look at how generic AI models perform in contract analysis.

Generic AI models, based on generative AI technologies, are trained on vast datasets of contracts, case law, and regulatory frameworks. This data is generally available on the internet, and is generally not specific to any industry or region. Generic AI can efficiently:

- Identify risky clauses and flag potential red flags.
- Provide general contract reviews and highlight inconsistencies.
- Suggest alternative language for better compliance.
- Extract key contract metadata for better lifecycle management.
- Automate contract categorization and summarization.

FIGURE 1. The Symphony of AI Agents: Harmonizing Intelligence for Contract Precision



These AI applications speed up contract review, reduce human effort, and enable legal teams to focus on high-value tasks.

Example: Lease Agreements

Consider a multinational company leasing office spaces across different countries. AI can identify standard risks in lease agreements, such as termination penalties, maintenance obligations, and liability limitations.

Example: Employment Contracts

A company expanding to different regions might use AI to review employment agreements. AI can flag basic compliance issues, such as missing termination notice periods or unclear confidentiality clauses.

The Limitation: Local Laws, Industry-Specific Regulations, and Company-Specific Policies

AI functions in a way that closely resembles human experience. When faced with an unfamiliar situation, a person with no prior exposure is likely to hesitate, struggle to make an informed decision, and remain uncertain about the outcome.

Similarly, AI operates based on the data it has been trained on – when it encounters a scenario it has not seen before, it becomes blindsided, unable to provide accurate insights or make the right decisions.

One such challenge arises in contract governance, which is far from uniform across the world. Legal frameworks differ by jurisdiction, and every organization has policies for compliance, risk management, and negotiation.[4]

If an AI system is not explicitly trained on these nuances, it will lack the necessary context to deliver reliable outcomes, often leading to incorrect or incomplete recommendations.

Let's take a closer look at the specific areas where AI tends to struggle:

- **Jurisdiction-Specific Compliance:** Certain contractual clauses may be legal in one region but prohibited in another. For example, non-compete clauses are largely unenforceable in California but permissible in other U.S. states.

- **Industry-Specific Regulations:** Healthcare, finance, and insurance sectors have strict compliance requirements that generic AI may not fully understand.
- **Company Policies and Internal Guidelines:** Organizations often have internal negotiation guidelines, preferred contract terms, and risk thresholds that a standard AI model does not natively understand.

Example: Healthcare Contracts

A hospital network using AI to review vendor contracts may need to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) in the United States. AI can help flag standard data protection clauses.

Still, it might not understand the nuances of specific state-level regulations. For example, California's stricter privacy laws under the California Consumer Privacy Act (CCPA) may impose additional compliance requirements that generic AI wouldn't automatically detect.

Example: Banking Agreements

A financial institution reviewing loan agreements across different countries might encounter issues where AI lacks localized insights. A loan clause that is permissible in Singapore might be restricted under European financial regulations due to stricter consumer protection laws. AI models must be trained on such distinctions to ensure accurate risk assessment and compliance.

The Solution: AI-Augmented with Custom Training/Prompting (Contextualize)

To address these limitations, we propose an advanced AI system – an early form of agentic AI that seamlessly integrates the broad capabilities of LLMs with specialized AI modules designed for targeted tasks. While LLMs excel at general understanding, they often require additional guidance to effectively perform domain-specific or context-driven tasks.

The approach leverages a network of AI agents, each serving a distinct function while maintaining the ability to exchange information dynamically. At the core of this system is a primary AI agent responsible for orchestrating interactions between various specialized agents.

This primary agent not only processes high-level queries, but also can train, configure, and set system prompts for supporting AI modules, ensuring a more tailored and efficient response generation process.

Like instruments in an orchestra, each AI agent plays a distinct role – company and regulatory policy, jurisdiction alignment – while the orchestrator AI conducts them in real time. Together, they transform fragmented insights into a seamless, adaptive contract intelligence system.

This AI architecture involves multiple layers of intelligence and adaptability:

- *Baseline AI Analysis:* The system leverages LLMs to perform a general contract review and risk assessment, providing an initial understanding of contractual obligations, clauses, and potential risks.
- *Custom Policy Training or Prompting:* Users can upload local laws, industry regulations, and company policies, allowing the AI to adapt to specific compliance requirements. These inputs help refine the system's decision-making process and ensure it aligns with legal and organizational standards.
- *User Validation and Fine-Tuning:* The system enables legal teams to review AI-generated insights, validate recommendations, and refine outputs over time. This iterative feedback mechanism ensures that the AI understands the nuances of specific policies and business contexts.
- *Continuous Learning Mechanism:* A built-in feedback loop integrates user input to enhance AI accuracy, improve decision-making, and continuously evolve its understanding of contracts and regulatory frameworks.

By implementing this structured AI ecosystem, we create a more intelligent, responsive, and scalable solution that effectively bridges the gap between general AI understanding and domain-specific expertise, empowering organizations with greater control, compliance, and accuracy in contract analysis and management.

Practical Use Cases

Jurisdiction-Specific Law: Construction Contracts

A construction firm operating in different states within the United States may need AI to review agreements with subcontractors. AI can detect missing indemnity clauses or unclear payment schedules. However, each state has different lien laws[5] affecting contractor payments. Without training or prompting on these specifics, AI might not provide the right recommendations for compliance.

Industry-Specific Regulations: Clinical Trial Service Agreements

A healthcare research organization may use AI to review clinical trial service agreements with external research partners. While AI can identify missing confidentiality or indemnity clauses, it may not be equipped to ensure compliance with regulatory frameworks like HIPAA or FDA

21 CFR Part 11 (67% of healthcare organizations are unprepared for the stricter security standards in HIPAA compliance-HIPAA Compliance AI in 2025).[6]

For example, generic AI models might overlook the issue if a contract omits specific language around electronic record retention or patient consent under these frameworks. Without domain-specific regulatory training, the AI may miss compliance gaps that could put trial data integrity or patient privacy at risk.

Company Policies and Internal Guidelines: Procurement Contract Reviews

An enterprise undergoing digital transformation may use AI to evaluate procurement contracts for alignment with internal spend governance policies. While AI can flag missing termination clauses or non-standard payment terms, it might not recognize violations of the company's specific approval thresholds or diversity sourcing mandates.

For example, if a contract bypass required review steps for purchases over a certain dollar value or lacks language supporting ESG vendor policies, generic AI would not raise concerns unless it is tuned with the organization's internal procurement policy framework.

Federal Procurement Policies: U.S. Federal Acquisition Regulations

Another critical domain where generic AI systems may struggle is federal government procurement, which imposes far more stringent compliance requirements than typical private-sector contracts. In the United States, the *Federal Acquisition Regulation (FAR)* serves as the primary framework governing contracting for most executive branch federal agencies establishing standardized procedures to promote transparency, fairness, and legal accountability.

As described in the examples discussed earlier, AI models used to review contracts in this space often lack the contextual understanding needed to enforce *FAR*-specific provisions. A general-purpose AI may overlook required flow-down clauses, Buy American Act requirements, or socioeconomic set-aside obligations.

For example a clause referencing subcontractor obligations under FAR 52.244-6 (Subcontracts for Commercial Products and Commercial Services) may be absent or improperly structured in a vendor agreement and remain undetected without *FAR*-specific training.

Moreover, the situation becomes even more complex when contracts must comply with *FAR* supplements such as *DFARS (Defense Federal Acquisition Regulation Supplement*). Without explicit training or prompting on these regulatory frameworks, AI-driven contract reviews risk serious consequences, including noncompliance, contract disputes, audit failures, or even legal penalties.

By incorporating *FAR*-specific rules and agency supplements into AI models either through fine-tuning or policy-driven prompting, organizations can improve the reliability and accuracy of AI systems when reviewing federal procurement documents, aligning them with the unique expectations of public-sector contracting.

Conclusion

While AI revolutionizes contract management, its effectiveness is limited by jurisdictional, regulatory, and company-specific nuances. The next step in AI-powered contract intelligence is integrating local laws and company regulations into LLMs, enabling businesses to harness the power of AI while ensuring full compliance.

By building a hybrid model that combines AI with tailored policy training/prompts, we can transform contract management into a more intelligent, adaptable, and legally compliant process.

This approach will not only streamline contract analysis but also provide businesses with confidence that their contracts align with both legal requirements as well as jurisdictional, regulatory, and company-specific nuances, reducing risks and ensuring smoother operations. CM

Niraj Ittan is a seasoned expert in contract automation and artificial intelligence, with a focus on driving innovation at the intersection of legal technology and intelligent systems. He brings over 18 years of experience in implementing solutions across the quote-to-cash domain and has successfully led more than 50 contract lifecycle management (CLM) implementations for organizations across various industries.

ENDNOTES

1 Martin, L., Whitehouse, N., Yiu, S., Catterson, L., & Perera, R. (2024). Better Call GPT: Comparing Large Language Models Against Lawyers. arXiv : https://arxiv.org/abs/2401.16212

2 Dataversity : https://www.dataversity.net/generative-ai-vs-traditional-ai/

3 Harvard Business Review : https://hbr.org/2024/12/what-is-agentic-ai-and-how-will-it-change-work

4 Stanford Law School : https://law.stanford.edu/2025/03/21/navigating-ai-vendor-contracts-and-the-future-of-law-a-guide-for-legal-tech-innovators/

5 *Construction lien laws can vary significantly from state to state,: https://www.sunraynotice.com/blog/understanding-the-complexities-of-construction-liens-types-of-lienors-and-exemptions*

6 HIPAA Compliance AI in 2025: Critical Security Requirements You Can't Ignore : https://www.sprypt.com/blog/hipaa-compliance-ai-in-2025-critical-security-requirements

FUNDAMENTALS OF CONTRACT MANAGEMENT

Contractor Team Arrangement (FAR Part 9)

BY JIM KIRLIN, CPCM, CFCM, NCMA FELLOW

A guiding principle of the Federal Acquisition System is using contractors that demonstrate a current superior ability to perform (FAR 1.102(b)(1)(ii)). This includes evaluating prospective contractors that have formed contractor team arrangements. Part 9 Contractor Qualifications prescribes policies and procedures pertaining to contractor team arrangements. The chart below defines contractor team arrangements and describes the government's policies regarding them, including limitations.

Title	
Definition (9.601)	Contractor team arrangement, as used in this subpart, means an arrangement in which – (1) Two or more companies form a partnership or joint venture to act as a potential prime contractor; or (2) A potential prime contractor agrees with one or more other companies to have them act as its subcontractors under a specified government contract or acquisition program.
General (9.602)	(a) Contractor team arrangements may be desirable from both a government and industry standpoint in order to enable the companies involved to – (1) Complement each other's unique capabilities; and (2) Offer the government the best combination of performance, cost, and delivery for the system or product being acquired. (b) Contractor team arrangements may be particularly appropriate in complex research and development acquisitions, but may be used in other appropriate acquisitions, including production. (c) The companies involved normally form a contractor team arrangement before submitting an offer. However, they may enter into an arrangement later in the acquisition process, including after contract award.
Policy (9.603)	The government will recognize the integrity and validity of contractor team arrangements; provided, the arrangements are identified and company relationships are fully disclosed in an offer or, for arrangements entered into after submission of an offer, before the arrangement becomes effective. The government will not normally require or encourage the dissolution of contractor team arrangements.
Limitations (9.604)	Nothing in this subpart authorizes contractor team arrangements in violation of antitrust statutes or limits the government's rights to – (a) Require consent to subcontracts (see subpart 44.2); (b) Determine, on the basis of the stated contractor team arrangement, the responsibility of the prime contractor (see subpart 9.1); (c) Provide to the prime contractor data rights owned or controlled by the government; (d) Pursue its policies on competitive contracting, subcontracting, and component breakout after initial production or at any other time; and (e) Hold the prime contractor fully responsible for contract performance, regardless of any team arrangement between the prime contractor and its subcontractors.

Jim Kirlin, CPCM, CFCM, NCMA Fellow is the author/co-author of three books on contract management.