Being Watchmen:

Compliance Challenges for Contractors & Agencies Now

PROPRICER

↓

Sign Up for a Demo

Compliance is no longer an isolated component of Government Contracting work. Its tentacles now extend into nearly every dimension of each proposal.

From banning citizen surveillance systems to detecting unsecured cybersecurity systems, compliance standards around technology components have heightened significantly in recent years.

And rightfully so: The National Security Administration has determined that one million new malware threats are released online every single day.

Vigilant compliance doesn’t stop with tech. Today it also involves prioritizing technical value over lowest Contractor price, employee harassment over the status quo, and privacy laws over promotional targeting.

Contract Compliance could soon become its own business category, for the watchmen (and women) who have the talent. Here’s a sampling of the challenges both Contractors and Agencies face today.

1. FAR Clamps Down on Contractors' Use of Specific Telecommunications & Video Surveillance Services

The 2019 Huawei scandal's effects are far-reaching. The telecommunications behemoth is barred from doing business with U.S. companies as a result of creating citizen profiling and surveillance infrastructure with its hardware through 4G and 5G networks.

As a result, The Federal Acquisition Regulatory (FAR) Council now says "no" to Government Agencies and Contracting firms looking to use such equipment produced by Huawei and other like companies as a substantial component of any system involved in a Contract.

Initial prohibitions in 2019 prevented Agencies from buying these products or services through a new contract award or by renewing an existing Contract that specifies these systems or services—with few exceptions or waivers granted.

Beyond these restrictions, a new requirement insists that a Contracting offeror now state whether it uses restricted telecommunications or surveillance components in the performance of any contract with the government—not just a contract at hand. The vice is tightening.

If an offeror can prove that it hasn't used these goods or services in any of its past Government Contracts, then it isn't required to prove its innocence in a new Contract.

But if an offeror has used these components or services at any time, it must continue to comply with the initial mandate on each and every contract.

This all boils down to stringent and exacting reporting requirements that dictate a Contractor immediately inform a Contracting Officer on the Agency side if suspect components or services arise in any Contract review.

For example, if a Contractor discovers "suspect equipment" within a Contract that's in process, they must report within one business day, or be subject to penalties. Further, within 10 business days, that Contractor has to report all mitigation actions—or efforts to replace or prevent use of the banned equipment.

Net/net: Contractors have to continuously review their entire supply chains for the presence of banned equipment or services and ensure they aren't components of government deliverables.

And this just passed: A government-wide ban insists Contractors eliminate the offending surveillance and telecommunications equipment from their entire scope of business operations—including their internal security, wireless, and VOIP systems. Looks like the Government means business on this piece of compliance. (1)

DATA PROTECTION

INTERNET SECURITY TECHNOLOGIES

2. New Amendments Sideline Agencies' Use of LPTA Source Selection Procedure

Not long ago, the Department of Defense (DOD) and the FAR Council amended the FAR to limit Agencies' use of the Lowest Price Technically Acceptable (LPTA) source selection process.

Basically, this means in the recent past the Government may have often compromised technical value when awarding a contract to an offeror from a league of competitors—a decision based on little more than lowest price.

Regulators and compliance bodies have long criticized Agencies' use of LPTA, which is often referred to as "a race to the bottom."

Now, Military Agency Contracting officers can use the LPTA process only when certain technical, performance-based criteria beyond cost are met. Officers also have to avoid "to the maximum extent practicable," using the LPTA process if a procurement is mainly to obtain:

- IT and cybersecurity services, systems engineering and technical assistance services, advanced electronic testing, or other knowledge-based professional services
- Personal protective equipment
- Training or logistics services in contingency operations
- Operations outside the United State, including Afghanistan and Iraq.

Civilian Agency Contracting officers are now under the same limitations as in the list above, but with the addition of:

- Audit or audit readiness services
- Health care services and records, and
- Telecommunications devices and services.

For many Contractors, these rules are a savior to their businesses—persuading Agencies to consider a Contractor Proposal's demonstrated technical merit over price alone. (1)

3. Rise of Cybersecurity Qui Tam Breaches, Calling for New Cybersecurity Standards

Cyberattacks on the Government have escalated exponentially in recent years, leading to laser-like focus on attack prevention and information protection. These efforts have, in turn, led to increased enforcement by Agencies concerning Contractors' noncompliance with cybersecurity regulations.

As one example, a company recently settled a qui tam lawsuit with the New York Attorney General that alleged the company's software, which was designed to control security camera systems, had flaws that rendered the system vulnerable to hackers.

The lawsuit alleged that the company was aware of these flaws and failed to disclose them after selling the software to U.S. state governments and the federal government (including every branch of the U.S. military).

Similar lawsuits contend that other Contracting companies are fraudulently entering into contracts with the federal government, despite knowing that they don't meet overall DFARS cybersecurity compliance requirements.

These cases are the first times courts have found allegations of noncompliance with a cybersecurity standard to form the basis of liability. (1)

Concurrently, the DoD knows that several recent high-profile breaches have made the current acquisition system especially risky for Agencies.

When Contractors deliver individualized cybersecurity plans as part of their respective proposal processes, the level of security hygiene varies wildly, because until now the Contracting companies have been self-certifying.

By creating a unified set of standards for cybersecurity, the DoD program intends to designate maturity levels ranging from "Basic Cybersecurity Hygiene" to "Advanced."

Contracting officers are now required to assess which level is required for each procurement and to include that level in the solicitation. As an ongoing set of guardrails, the DoD plans to modify the levels on a yearly basis to ensure cybersecurity controls remain current as cyber threats evolve.

From now on, a third-party auditor must certify a Contractor, who will evaluate the Contractor's cybersecurity hygiene and certify (or not) that Contractor at a specific level.

Importantly, there are no exceptions for small businesses, commercial products, or whether a Contractor will ever possess Controlled Unclassified Information (CUI) or not while performing a contract.

All Contractors and Subs must be cybersecurity-certified for each and every contract. And that's that. (1)

↓

Book Demo

4. CFIUS Review Process of Foreign Investments Could Significantly Expand in Scope

When it comes to foreign investment in U.S. companies that have federal Agency contracts, the winds of change are currently blowing. New rules also apply to foreign companies that own U.S. companies involved in contracts.

The main instigator? The Committee on Foreign Investment in the United States (CFIUS). Once the Foreign Investment Risk Review Modernization Act (FIRRMA) passed, the scope of monetary transactions involved in Contracting companies that are reviewed by CFIUS just keep on growing.

Spotlights include the following:

- Active investments by foreign entities are reviewed under certain circumstances. In broad brushstrokes, investments in companies that house critical tech nology, involve critical infrastructure, or hold U.S. citizens' personal data, will be under scru tiny soon.

- Specific real estate transactions are now subject to review. CFIUS will review all property that's situated within one mile of a U.S. military station.

- Investments that include substantial monies from foreign governments are subject to audit. Proposed regulations contain a "white list" that would outline foreign investors who are exempt from CFIUS requirements. All other firms and their investments will be studied closely.

Contractors with foreign holdings or investments that may be subject to these new requirements should continuously and monitor ever-changing CFIUS regulations to be sure they remain compliant. (2)

5. Political Shifts Causing Regulatory Changes

Trump's tenure in the Oval Office initially brought widespread regulatory rollbacks. Now, after Compliance changes have been incrementally implemented, the tides will change yet again with Dems in control of … well, everything.

But even the initial shifts to the Right may not have a major impact from a legislative and regulatory standpoint. Although the most recent political changes are sure to stall final implementation of a deregulatory agenda—and then another rollback—real regulatory change moves like a turtle and still rests in the hands of the Agencies.

But don't ignore international regulatory and political

events. The European Union's General Data Protection Regulation (GDPR), which took effect in 2019, has reach beyond Europe. It also serves as a model for future possible U.S. regulations in the critical areas of data privacy. California has already implemented such measures for tech firms, through its California Consumer Privacy Agenda (CCPA).

Any Contracts involving internal or external websites that capture privacy information, or inbound or outbound demand-generation programs, need to include mechanisms to address both GDPR mandates and, in California, CCPA mandates. (3)


CONTRACT

A legal entity registered under the laws of Russia, hereinafter "the Firm", in the person its General Director, and a legal entity registered under the laws of hereinafter "the Client", in the person of its Managing Director, acting on the basis of the charter concluded the present Contract which entered into force on the date of signing as follows:

1. Subject of the Contract

1.1 The subject of the present Contract shall be the providing of legal services by the Firm to the Client, which shall be paid by the Client in accordance with the invoices issued by the Firm on the basis of the hourly rates of the Firm's personnel multiplied to the quantity of the hours spent by them.

2. Payment for services

2.1 The hourly billing rate of the personnel of the Firm vary from 100 to 200 USD per hour excluding VAT. However, upon the request of the Client the Firm can preliminary estimate the cost of certain services and inform the Client about the cost of prospective services.

2.2 As documentary certification of final acceptance of services an Acceptance Act shall be drawn up (hereinafter "the Acceptance Act") to be signed by both Parties. The Acceptance Act shall be signed by the Client within 5 business days from the moment of submission by the Firm.

2.3 Acts of Acceptance, invoices and other settlement documents of the Firm shall be drawn up in US Dollars, and the Client's payment documents shall be drawn up in US Dollars. Actual settlements under the present Contract shall be effectuated in US Dollars.

2.4 The Client shall pay Firm's invoices within 10 business days from the date of their receipt.

SIGNATURE _____

6. GSA Schedule Contract Obligations

General Services Administration (GSA) schedule Contracts offer both Agencies and Contractors broad business opportunities but come with special compliance obligations. They include pricing, discounting, labor categories, and disclosures—and require constant monitoring.

- **Scope Compliance.** Contracting companies can only deliver the specific products and services that the GSA has authorized for sale under your Schedule contract. Others? Nope.

- **Invoicing Compliance.** GSA Schedule Contract projects have unique invoicing requirements, such as prompt payment terms, inclusion of GSA contract numbers, and others.

- **Teaming Compliance.** Two or more GSA Multiple Award Schedules (MAS) Contractors can work together in order to meet Agency requirements under a Contractor Team Arrangement (CTA). This is especially lucrative when another Contracting firm complements yours. You can then join forces for proposals you might not qualify for on your own.

- **Trade Agreement Act (TAA) Compliance.** Under your GSA Schedule Contract, you agree to provide the Government with only U.S.-made or TAA designated country products, as part of your deliverable performance.

- **Labor Qualification Compliance.** If your firm delivers professional services as part of a Contract, the people you provide under each GSA task order have to meet minimum qualifications as specified in your GSA MAS contract. (4)

PROPRICER

7. Be Ethical. Be Honest: Contracting Compliance Around Business Ethics

Federal Government Contractors must “conduct themselves with the highest degree of integrity and honesty,” and have a written code of conduct in place.

Additionally, any company hoping to compete on Contracts at a Federal level must now conduct employee business ethics and compliance training classes—and put an internal control system in place to make sure the learnings stick.

These programs have to:

- Scale to the size of the company and the extent of its involvement with the government
- Ensure quick discovery and disclosure of improper conduct, and
- Not let corrective measures slide.

This compliance program has to be spelled out in a Contract if its value is expected to exceed $5.5 million and the performance period is 120 days or more.

For all Contracting firms:

- The code of business ethics and conduct must be made available to Contractor employees within 30 days of award of a covered contract.
- You must exercise due diligence to prevent criminal conduct and promote an organizational culture that encourages a commitment to compliance with the law.
- You have to disclose in writing if you have credible evidence that a principal, employee, agent or subcontractor has committed a violation of criminal law involving fraud, conflict of interest, bribery, or gratuity violations or a violation of the civil False Claims Act.

It pays to stay on the right side of general business ethics, especially when dealing with Government Agencies. In many cases, it can pay very handsomely. (5)

8. Contractor Compliance in the Era of #MeToo

Sexual misconduct allegations are now rampant in the media and entertainment industries, and unfortunately, also in Congress.

Many incidents involve breach of the Civil Rights Act of 1964. Others involve civil and criminal accusations of a much more serious nature.

While usually not headline-making, Contractors can face allegations, just as anyone in business or Government today can.

Harassment falls under the Equal Employment Opportunity Commission (EEOC) and court jurisdiction as a form of sex discrimination.

The statutory basis for a sexual harassment complaint makes it an unlawful Contractor practice for an employer to discriminate against an employee or applicant for employment on the basis of sex, and in many cases, sexual orientation.

In the context of Government Compliance, there are two types of sexual harassment. One is known as “quid pro quo” harassment, where submission to such harassment is made a condition of an employee’s employment. The other type is a hostile work environment, such as a place where demeaning comments about one’s gender are made and tolerated in the workplace.

Today, this is what constitutes harassment, in the eyes of Government Agencies:

- Unwelcome advances, requests for favors, and other verbal or physical harassment.
- Offensive remarks about a person’s sex. For example, it is illegal to harass a woman by making offensive com ments about women in general.
- Both victim and harasser can be either a woman or a man, and the victim and harasser can be the same sex.
- When it comes to teasing, offhand comments, or isolated incidents that are not serious:
  These actions are illegal when so frequent or severe they create a hostile or offensive work environment or when they results in an adverse employment decision (such as a victim being fired or demoted as retaliation for com plaint—which is, in itself, another violation and cause for a Contractor’s suspension or non-award, not to mention potential civil or criminal prosecution).
- The harasser can be the victim’s supervisor, a supervisor in another area, a co-worker, or even a client or prospec tive customer. (6)

The short of it: Compliance can now encompass such intangibles as your employees’ behavior, your preference for savings over quality, and even your penchant for hiring certain types of personalities over others. Watchmen and -women, remove any masks of indifference. True compliance is on all of our watches.

Sources:

1. The Top 10 Compliance Challenges of 2020 Report

2. Thomson Reuters: Regulatory Intelligence Blog – Top Concerns of U.S. Compliance Officers

3. Attila Security Blog: Compliance Challenges Facing Government Contractors

4. Crowell Moring Blog

5. Compliance Insights Website: How to Navigate Unique Risks and Rules

6. Cherry Bekaert Guidance Article: #MeToo and Federal Contractors

PROPRICER

www.propricer.com