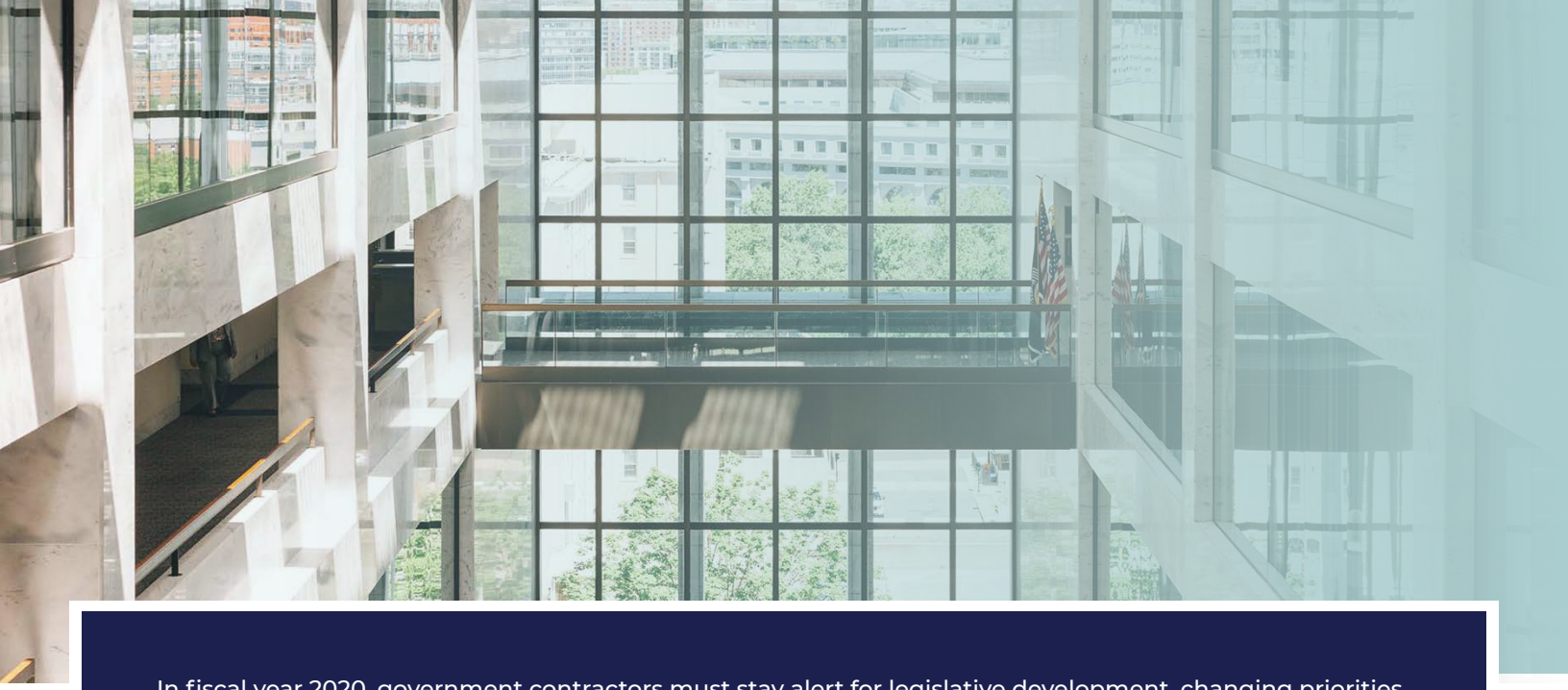
GOVERNMENT CONTRACTING IN 2020:

Protecting Data Integrity

wj technologies



In fiscal year 2020, government contractors must stay alert for legislative development, changing priorities, and technological trends that impact their company and industry, especially with regards to cost reporting and compliance.

2019 saw increased government oversight and operational risks, and this trend is likely to continue. As a result, it is increasingly important for government contractors to invest in modernized infrastructure that integrates and automates processes, especially those related to data collection, storage, and cybersecurity.

We are outlining what government contractors must know in terms of legislation, cybersecurity, and supply chain management, to meet and surpass federal standards in 2020.

LEGISLATION

In 2019, the Defense Contract Audit Agency (DCAA) significantly reduced their Incurred Cost Submission backlog by contracting with independent public accounting firms to perform these audits, giving DCAA more time for other types of audits.

Incurred Cost Submissions

Contractors must be increasingly careful to bill the government only incurred costs that are allowable according to the Federal Acquisition Regulation (FAR) rules. Allowable costs typically include fringe benefits, maintenance and repair, professional services, and more. Meanwhile, non-allowable costs include but are not limited to entertainment, fines and penalties, and lobbying initiatives.

Among the new audits that contractors must be ready for are proposal audits to identify where incurred costs may factor into future contracts, and accounting system audits to ensure that their accounting system meets “Generally Accepted Accounting Principles” and compliance criteria, including cost segregation.

Data Privacy

Perhaps more importantly, data privacy continues to become increasingly important to both the public and private sectors. By now, many consumers are aware that the California Consumer Privacy Act (CCPA)—a framework similar to Europe's General Data Protection Regulation (GDPR)—has gone into effect in California. What's more, the National Institute of Standards and Technology (NIST) recently released a draft Data Privacy framework, and we can expect updates this year.

Although government contractors are already required to follow the FTC's safeguard rules to protect confidential information, there have been no updates to the regulations since 2003. New amendments released for public comment last fall will take effect this year, with primary regard to documenting an adequate information security program, and new requirements for encryption, multi-factor authentication, and secure development practices to ensure adequate security in the new decade.

As a result of the new regulations, we highly recommend investing in Enterprise Resource Planning (ERP) software like Costpoint, Unanet, and Jamis. Unlike Quickbooks, which has significant limitations for government contractors and growing enterprises, ERPs are scalable accounting software platforms that allow for more functionality and automation. More importantly, ERPs are designed to support government requirements like those mandated by the DCAA for time tracking, projects, expenses, and labor distribution.

CYBERSECURITY RISK

In 2020, government contractors and other groups that receive federal dollars must plan to tighten up security standards to comply with the Cybersecurity and Infrastructure Security Agency (CISA) 's Cybersecurity Framework while protecting personally identifiable information (PII) for clients and customers. Government contractors must be ready to invest in digital hygiene training as an act of good faith in the prevention of threat incidents.

Specifically, contractors and organizations must be prepared to demonstrate compliance with controls in the following categories: Identify, Protect, Detect, Respond, and Recover. By developing a comprehensive information security program, contractors can minimize the likelihood of increasingly prevalent cybersecurity risks like ransomware attacks that affect everything from businesses to local governments and the impact of sophisticated phishing attacks and vulnerabilities in the supply chain.

Fortunately, employing seemingly simple digital safety practices can prevent most security incidents and insider threats. Training users to click only safe emails, use passwords to protect devices, and leave data storage onsite can fend off most threats before they happen.

Cybersecurity Maturity Model Certification (CMMC)

Moreover, defense contractors must prepare for the upcoming rollout of the newly released Cybersecurity Maturity Model Certification (CMMC), which uses a scale of 1-5 to rate a government contractor's technical practices and process maturity.

Prior to CMMC, to be awarded future contracts, contractors had to demonstrate compliance with government cybersecurity regulations. Although this has always been the expectation, actual compliance has not been commonplace. Under CMMC, contractors must achieve a specific CMMC rating (typically 1-5) from an outside qualified CMMC auditor before a contractor can be awarded a solicitation or a project by the Department of Defense (DoD).

Although CMMC specifically governs DoD contractors at this time, it will likely expand to other contractors as well, if not this year, then in the coming years.

SUPPLY CHAIN MANAGEMENT

In 2019, tech vendors fell under scrutiny from the current administration and industry professionals throughout the federal government. The CMMC rollout, explored in the Cybersecurity Risk section of this ebook, helps organizations to make better decisions for IT acquisition while mitigating supply chain risk.

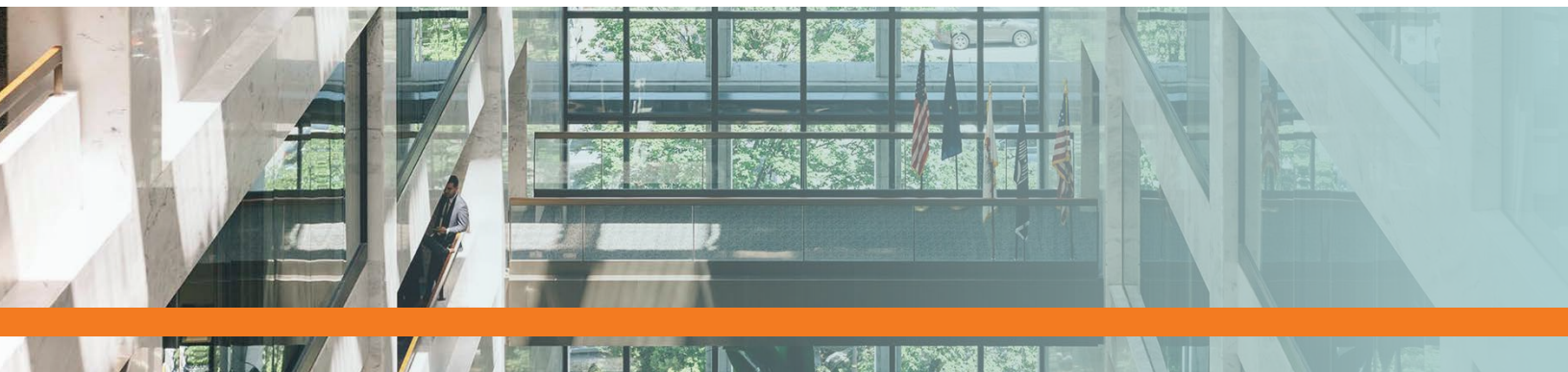
The Internet of Things (IoT) products, in particular, suffer from a lack of basic security controls. NIST is preparing legislation to address this issue, but in the meantime, organizations should be wary of the IoT in general and segment IoT products from their main networks.

Another example of supply chain risk might be a product vendor who does not provide End-of-Life (EoL) support due to either policy or the end of a product's service life.

Legislation signed into law last summer (EO 13873) addresses the risk of products that may provide backdoors for foreign countries. It expressly states that organizations may not use information technology products from vendors considered a "national security risk" under any circumstance.

Contractors can and should step up their vendor risk strategy by complying with security regulations, but also by implementing quality control criteria like those set by the National Information Assurance Partnership (NIAP), which ensures that products meet U.S. cryptography standards, and the International Organization for Standardization (ISO), a certification verifying that products meet a high standard.

By choosing the right business partners with appropriate CMMC maturity, government contractors will have an advantage while also ensuring business integrity and product quality.



PUTTING IT ALL TOGETHER

Technology has developed rapidly over the past decade, and the legislation is finally catching up. In preparation for the new decade, government contractors must be prepared to make rapid changes in response to continued developments.

Government contractors can and should invest in three main areas to ensure prime readiness for adjusting to new technologies and regulations.

Improved Accounting Systems

While programs like Quickbooks are suitable for small businesses, we often find that this type of software is not sufficiently robust for growing enterprises. Instead, most of our clients' experience cost savings, improved data integrity, and can more easily comply with government regulations when they implement an ERP.

Risk Assessments and Modernization of IT Infrastructure

Training personnel in best practices for cyber hygiene is no longer a "should" it's now a must. Instituting simple practices and standards prevents needless breaches and security incidents and is the first step in mitigating cybersecurity risk. In addition to training, when contractors must take the time to identify the areas with risk potential and developing a response plan, only then can they begin to update their IT infrastructure.

Vetting and Accountability for Supply Chain Partners

Ultimately, a company will be held accountable for the partners it chooses, so contractors must invest in ensuring that vendors and subcontractors—or supply chain partners—meet or surpass the highest standards and are compliant with government regulations. It's the law for federal contractors, but it's also good business.

Companies that invest in these areas are more likely to achieve success and be awarded more lucrative government contracts. Furthermore, they'll be the best prepared to weather any changes this decade brings.

Government Contracting in 2020:

Protecting Data Integrity

What government contractors must know in terms of legislation, cybersecurity, and supply chain management, to meet and surpass federal standards in 2020.

LEGISLATION

- [ ] Incurred Cost Submissions
- [ ] Data Privacy

CYBERSECURITY RISK

- [ ] Cybersecurity Maturity Model Certification (CMMC)

SUPPLY CHAIN MANAGEMENT

- [ ] Review Recent Legislation
- [ ] Develop Vendor Risk Strategy

Government contractors can and should invest in **three main areas** to ensure prime readiness for adjusting to new technologies and regulations:

1. Improved Accounting Systems
2. Risk Assessments & Modernization of IT Infrastructure
3. Vetting & Accountability for Supply Chain Partners

WJ Technologies combines years of experience in accounting and accounting systems with a genuine desire for our clients' success. Allow us to help you find the perfect solution for your organization. If you are considering an upgrade to your accounting system, please contact us to talk about the next steps.

We look forward to hearing from you!

950 Herndon Parkway
Suite 430
Herndon, VA 20170

T: 703.885.8170
F: 703.885.8171
E: info@wjtechnologies.com

wijit
wj technologies