



Technical procurement and compliance: Navigating the processes and regulations for federal government

Procurement in the U.S. government can be a complex process with many different processes to follow. Similar to other businesses, the federal government acquires a diverse range of goods and services, ranging from real estate to surveillance and office equipment. However, the procurement process adheres to specific protocols, making the intricacies of technical procurement challenging to comprehend. Fortunately, with the proper procedures in place and the right guidance, navigating the ins and outs of this process becomes much simpler for all parties.



Breaking down the procurement process

U.S. federal agencies are required to adhere to unique regulations that govern processes of all scales and complexities. Whether carrying out the minutiae of day-to-day operations or completing large-scale projects, government agencies are subject to more threats and risks than most other organizations. This elevated profile demands very specific and sometimes complicated protocols.

When it comes to technical procurement, there are strict requirements constantly being put in place surrounding information assurance, privacy compliance, and cybersecurity. However, the rapid pace of technological advancement sometimes outpaces government capabilities. With guidance, agencies can maintain up-to-date technical procurement requirements that protect the integrity of some of America's most vulnerable organizations.

It is imperative that all manufacturers, vendors, and interested agencies maintain their own strict compliance regulations that are in line with federal government restrictions, including the **Trade Agreement Act** (TAA) and the **National Defense Authorization Act** (NDAA). By staying up-to-date with current compliance requirements along with the U.S. government's **Federal Procurement Policy** (FPP), vendors have ample opportunity to secure federal government contracts for the supply of technology and other relevant products and services to federal agencies.



The technical procurement process

Agency leaders need to possess an in-depth understanding of federal procurement requirements and the contracts that exist between vendors and government agencies. Likewise, vendors and service providers vying for contracts with the federal government must also understand its often nuanced requirements. While the constraints can be hefty for both parties, they are relatively easy to adhere to once understood.



Bidding

The first step in procurement is to respond to government requests for proposals (RFPs) or requests for bids (RFBs). When an agency requires a product or service, it will typically release a request along with details provided by the Information Assurance Office that represents the agency. The Office is responsible for setting out the requirements for that particular contract.

Contracts are generally drawn up ahead of time and must follow relevant regulations put forth in the **Federal Acquisitions Regulations** (FAR) or by the **National Institutes of Standards and Technology** (NIST).

Federal agencies often participate in contracts that require a vendor to provide them with the tools they need to maintain physical security, operational efficiency, and employee safety. Prior to accepting a proposal, agencies must take precautions to ensure the vendor they're selecting can meet the tight requirements of working directly with the government. These steps usually include having the capability to ensure that technology is void of security vulnerabilities and providing automated firmware updates as required.

Procuring surveillance equipment

Surveillance equipment is a vital part of government security systems. While some government agencies like Customs and Border Protection understand the unique security requirements and potential complications of these tools, other agencies may find value in consulting with experts. By engaging a trusted consultant, agencies can access invaluable advice and guidance to procure secure system components effectively.

Federal agencies in search of third-party consulting services should seek out an authoritative company with extensive experience in supplying technology to the government. Acting as an advisor, the company should understand the potential security threats and risks commonly faced by the government, as well as the steps that federal agencies can take to prevent a breach.

It's important to note the restrictions and rules surrounding technical procurement that federal agencies must follow apply broadly to all areas. So, agencies procuring any technology must follow these regulations and work exclusively with vendors who can honor their end of the contract. While this list isn't exhaustive, some of the devices that agencies may need to procure while following FAR, TAA, and NDAA regulations include:

- > Video surveillance devices, including security cameras
- > Network audio systems
- > Sound detection systems
- > Network video recorders
- > Access control



Winning a bid

When a contractor gains the Authority to Operate (ATO) for their service or product, this means the device or service they're authorized to provide has passed a rigorous series of security tests. Testing is required for any technical devices or equipment in the ecosystem and, due to the high standards maintained by the federal government, any vendor with the ability to pass this testing is considered extremely safe when it comes to cybersecurity.



Critical compliance for surveillance

Two key pieces of legislation govern the process of sourcing new technologies for the federal government: the Trade Agreement Act and the National Defense Authorization Act. Failure to comply with these two acts will likely result in a breach of contract between the vendor and the government agency.

The Trade Agreement Act

The TAA governs the manufacture and distribution of products from foreign suppliers. Overseen by the **U.S. General Services Administration** (GSA), the TAA regulates the following technical products and services:

- > Cybersecurity products and services, including consulting
- > Data center services
- > Hardware products and services
- > Software products and services
- > Telecommunications and network services

In addition to the above, a variety of other **products and services** are required to comply with the TAA.

TAA Requirements

All products or services listed by the GSA must be manufactured or substantially transformed in either the United States or a TAA-designated country. Countries authorized by the GSA include Australia, Canada, Japan, Spain, and other signatories of the World Trade Organization Procurement Agreement and Federal Trade Agreement.

To obtain authorization to provide products or services to a government agency in the United States, contractors must certify that they're able to meet this requirement (known as the "rule of origin"). Several countries typically do not qualify for trade with U.S. government contractors,

such as Russia and China. If a contractor seeks an exception in order to do business with vendors in non-qualifying countries, they can petition U.S. Customs and Border Protection for an advisory ruling. This ruling may or may not permit contractors to import specific products from non-qualifying countries.

Close knowledge of TAA requirements is essential for contractors and representatives procuring technology for any federal agency. A breach of TAA rules can lead to civil and criminal liability as well as significant penalties.

The National Defense Authorization Act

The NDAA authorizes appropriations and expenditures for defense-related activities and applies to procurement activities within the Department of Defense (DoD) and the Department of Energy (DoE) nuclear weapons program. Reviewed and updated by Congress annually, the NDAA determines defense policies, restrictions, and organizational matters.

Section 889 of the 2019 NDAA addresses cyber threats and other technical risks, such as privacy breaches and espionage, in detail. It also outlines the risk associated with specific equipment and technologies, particularly those made by certain Chinese manufacturers. Section 889 further included an amendment to the FAR that prohibits executive agencies from working directly with vendors and contractors who supply or use specific telecommunications equipment.

Section 5949 from the 2023 NDAA establishes that an executive agency is prohibited from acquiring or renewing contracts for electronic parts, products, or services that incorporate covered semiconductor products. Additionally, Section 5949 elaborates that semiconductor products manufactured by certain Chinese technology companies that will be barred from U.S. defense procurement.

Regulatory compliance for government vendors and contractors

The above regulations reflect the federal government's concern for national security and should not be taken lightly. Authorized contractors who fail to comply with relevant regulations can face fines or even jail time, depending on the nature and severity of the infraction. By working directly with vendors who understand regulatory compliance, federal agencies can ensure a mutually beneficial relationship.

Both federal agencies and contractors should review annual updates to the TAA and the NDAA or FAR. Most importantly, agencies should be aware that purchasing telecommunications equipment manufactured in China, Russia, and other restricted countries is prohibited.



The importance of data protection and cybersecurity

Agencies should prioritize securing their network and devices to help mitigate any potential cyber threats.

An important standard for the federal government set by the U.S. National Institute of Standards and Technology (NIST) is the Federal Information Processing Standards (FIPS). FIPS standards apply to federal agencies that are using cryptographic-based modules to safeguard information security across their operations and assets. Ultimately, these standards help secure data confidentiality and integrity. There are four levels of security within the FIPS standards: Level 1, Level 2, Level 3 and Level 4. With each increasing level, there are more restrictive requirements. While mandated for U.S. and Canadian government use, they're also widely adopted internationally due to their recognition in other security standards.

Best practices for cybersecurity

Because high-value networks are frequently under attack, government agencies have been forced to strengthen their security infrastructure. Cyber hardening includes an in-depth analysis of entire networks and technology ecosystems to identify and patch existing vulnerabilities and is a vital tool in preventing cyberattacks. This process involves intense scrutiny of each aspect of a surveillance network, camera and other technical systems starting with the hardware itself and working outwards to the application layer. Hardening ensures that each layer of the device is secure, works with strong network protection, and connects to a redundant power supply.

All technical solutions must involve carrying out cyber hardening on every device supplied to the federal government. This is easiest when all devices work together in a holistic, living ecosystem that can be analyzed cohesively to ensure hardness across the entire network.



About Axis Communications

Axis enables a smarter and safer world by creating solutions for improving security and business performance. As a network technology company and industry leader, Axis offers solutions in video surveillance, access control, intercom, and audio systems. They are enhanced by intelligent analytics applications and supported by high-quality training.

Axis has around 4,000 dedicated employees in over 50 countries and collaborates with technology and system integration partners worldwide to deliver customer solutions. Axis was founded in 1984, and the headquarters are in Lund, Sweden.

For more information about Axis, please visit our website www.axis.com.

©2024 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC and VAPIX are registered trademarks of Axis AB in various jurisdictions. All other trademarks are the property of their respective owners.

