About The Gormley Group | Join Our Mailing List | Our Services

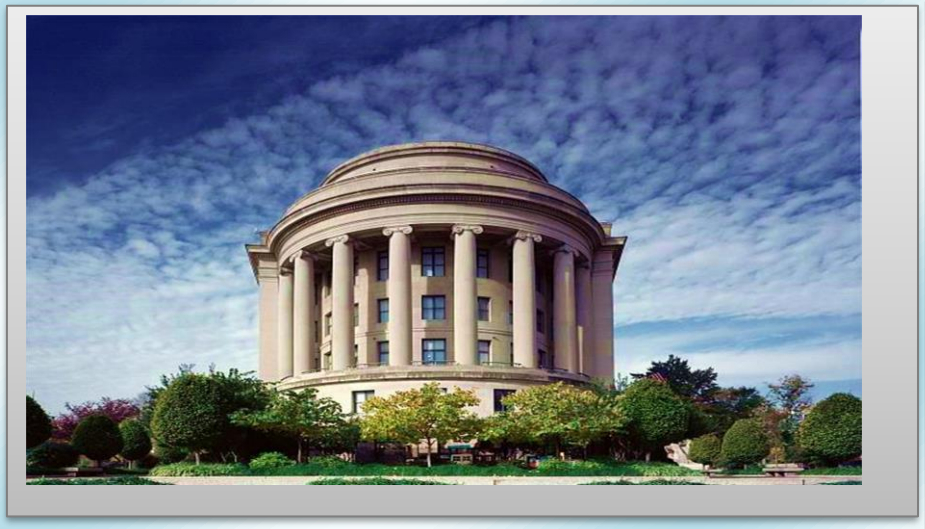
IN THIS ISSUE

QUICK LINK

Our Services
TGG Strategic Sales Planning
About The Gormley Group
Join our Mailing List

CONTACT

The Gormley Group
1990 M Street, NW
Suite 480
Washington, DC 20036
www.gormgroup.com
info@gormgroup.com



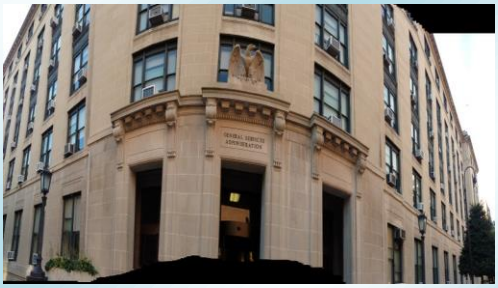
Domain Expertise

GSA Making Changes to its Federal Acquisition Service (FAS) Structure

GSA says the overall changes to the FAS structure are minimal, with the majority of FAS organizational units remaining unchanged and employees will not be moving duty stations or changing functions. GSA says the majority of current FAS organizational units will remain as they are, and those that are moving are primarily "lifts and shifts," with the teams remaining intact.

"Realigning FAS to the principles of category management is a critical step in fully integrating a more strategic and customer-focused business model across the agency," a GSA spokeswoman said in a statement to Federal News Radio. "To accomplish this, FAS undertook a strategic organizational realignment of our workforce and processes. The realignment plan supports FAS efforts to adopt the principles and vision of category management — helping the government to act as one — but also improves organizational efficiencies and effectiveness in the delivery of acquisition solutions and services."

Read More



Federal Marketplace Matters

Turner Roth: 18F hears IG's concerns but isn't losing long-term vision

The General Services Administration digital services team 18F will take the advice of a recent inspector general report to re-evaluate its balance of billable and non-billable work, GSA Administrator Denise Turner Roth told FedScoop Thursday. But that doesn't mean 18F will lose focus on its long-term mission to transform the way the federal government buys and builds technology, she said.

"18F in its short existence has showed how it can help the federal government and federal agencies, and how important its mission is," Turner Roth said. "But certainly, like other startups, it's not perfect. It has room to grow and areas to work on."

The GSA IG issued a report — sparked by the concerns of senior GSA official — in late October that called 18F out for continually failing to recover its costs, losing $31.7 million since it was founded in 2014.

Read More

GSA's Federal Acquisition Service: A Recap of FY2016

FY2016 recently came to a close, and I can't help but reflect on what a remarkable 12 months it's been for all of us associated with the Federal Acquisition Service. As I do at the start of every fiscal year, I'd like to reflect on what we've accomplished over the past twelve months. However, in this year's blog, I also want to look forward and share how we're building on this momentum.

When I was sworn in as the FAS Commissioner in February of 2013, I laid out a three-year goal for the organization: GSA should be recognized as the government acquisition marketplace. FY16 marked the final year of that 3-year FAS vision and I'm excited to share what we've accomplished to date.

Three years ago, we set out to build, operate, and maintain a governmentwide marketplace to generate savings, improve efficiencies, and deliver excellent customer service. But what does that mean exactly? It means we want FAS to be the provider of:

- Unbiased Advice: FAS will get you the best value, no matter where it comes from.
- Better Contracts: FAS will offer easy access customer-focused contracts that meet agency requirements.
- A Full Spectrum of Services: FAS will offer acquisition services that support every level of need, from agencies that want to do it all to those that need it all done for them.

Each of these game-changing initiatives was designed to better support our customers and our industry partners, while also letting us make the best decisions on behalf of the taxpayer. Today, I'm pleased to report that FAS has made great strides on a number of these objectives.

In the past three years, we've introduced many new initiatives to make the FAS Vision a reality. Among them is Category Management. Led by our partners in OMB's Office of Federal Procurement Policy, Category Management is the process of managing product or service categories as strategic business units and customizing them to meet customer needs.

Read More

Federal Marketplace Matters

Thiel's Palantir Wins Battle Over Army Combat Data System

"…A Palantir Technologies Inc. unit won a second chance at a contract to build the next phase of the U.S. Army's integrated combat data system, an undertaking potentially worth hundreds of millions of dollars.

The Army failed to adequately consider commercially available options for the system, effectively shutting out the Silicon Valley firm from bidding, a federal judge ruled on Monday. The judge barred the Army from awarding the contract and ordered it to restart the process of evaluating technology that already exists."

Read More

DHS gives its 'backlog' of contract closeouts a taste of the PIL

The Homeland Security Department's Procurement Innovation Lab (PIL) is tackling one of those hidden problems of federal acquisition — the need to close out low-risk, low-dollar contracts.

Too often these contracts are forgotten or under prioritized, and a backlog builds up. At DHS, for example, its backlog grew to more than 350,000, and 92 percent of the contracts had been completed more than a year ago.

Soraya Correa, the chief procurement officer at DHS, said the PIL took an innovation risk and re-engineered the business processes for contract closeout.

Correa said the PIL developed new quick closeout procedures in a simplified manner. DHS released a Federal Register notice in early October alerting contractors of its plans and the requirement to submit all outstanding invoices by Dec. 2.

"I'm talking about contracts that are typically small dollar value, generally firm fixed price, no activity over the last 12-to-24 months, final goods and services have been delivered so we know they are probably ready for close out," Correa said in an exclusive interview with Federal News Radio. "What we are doing is a streamlined approach trying to close them in one fell swoop."

Correa said the PIL brought together a team of experts, from the CFO's office to contracting to auditors to industry, to develop these new processes.

"Once the contract is completed, we make sure the final invoice has been received and has been paid. We identify if there are any leftover funds on the contract or any action that has to be taken. We confirm with the parties involved, the program office, the contractor and the contracting officer that there are no further actions, and then we do a modification to close out the file and retire that contract file," she said. "These steps can be a little bit tedious because sometimes you have to go out and do some research. You may have to research in the financial systems. You may have to research with the program office, and even sometimes the vendors have to do research."

Read More

Federal Marketplace Matters

Federal Government Revises Its Big Plans for Little Tech

A group of federal agencies think nanotechnology could help them do their jobs better, and have resolved to invest more in its development.

Earlier this week, the National Science and Technology Council updated its strategic plan for nanotechnology research and **investment**; that document, updated every three years, outlines various goals including committing to host more related contests and challenges.

The roughly 20 agencies mentioned in the plan make up the National Nanotechnology Initiative—a governmentwide collaboration that has so far invested about $23 billion in research and the "responsible transfer of nanotechnology-based products from lab to market."

Read More

Pentagon Pleads With Contractors to Step Up Fight Against Industrial Espionage

A long-feared flow of Chinese-made counterfeit electronic parts and malicious software is making its way into the assembly lines of U.S. defense contractors. The Pentagon's nightmare scenario: An orchestrated campaign to not only sabotage U.S. weapon systems but also steal sensitive design data from American companies.

It is a wide open secret that the Pentagon's complex supplier base has become a huge target.

"We see growing opportunities for bad people to get at our products," said Undersecretary of Defense Frank Kendall, who oversees weapons acquisitions.

Kendall noted that this threat has lurked for decades, "as long as I've been in government," he said Oct. 26 at an industry forum hosted by Bloomberg Government. But only in recent years has the Pentagon seen substantial data and evidence of cyber attacks, tampering and other nefarious actions aimed at the defense industry. Without naming names, Kendall said there are mounting concerns about "things that are hidden in the things that we buy."

The security gaps have widened over time, resulting from a combination of economic and technology trends — the globalization of electronics supplies and proliferation of counterfeits, the internet of things and the widespread use of software in military systems. The prospect of malicious tampering has become all too real, said Kendall. "What is my greatest fear? That we'll find one day when we ask our systems to do something, they won't work."

These issues fall under the broad category of "supply chain security," and they have put the Pentagon in a tight spot because it has limited visibility and control of the vast web of suppliers that design and produce equipment for the military.

Read More

Federal Marketplace Matters

Scott unveils federal open source site: Code.gov

Federal CIO Tony Scott revealed a new public open source website housing the custom code for a number of digital projects the federal government is currently developing.

The site, Code.gov, aims to capitalize on open source push by the Obama administration to share custom code across federal agencies and the public.

The move comes after the August release of the Federal Source Code Policy, requiring federal agencies to share their custom code for digital projects with each other, as well as 20 percent of it to the public.

The new site, which launched on Nov. 3, provides that public destination for citizens to watch and help influence the development of digital projects meant to improve federal services.

Read More

Educational

Defense Contractor Cybersecurity Breaches Bring Wave of Cyber Whistleblower Opportunities

Failure to report cyberattacks among Department of Defense (DOD) contractors and subcontractors means big whistleblower opportunities for IT professionals and other defense contractor employees. Cyber hacking and cybersecurity breaches are widespread, and a whole new category of cyber whistleblower claims are cropping up around them under the federal False Claims Act.

Cybercrime could cost U.S. Companies $2 Trillion by 2019

Cybercrime cost U.S. companies approximately $500 billion in 2015. This number could quadruple to $2 trillion by 2019. Cyber hacks into the computer networks of private vendors that supply aircraft, ammunition, radar technology and specialized software to all areas of our U.S. defense agencies present a significant danger to national security and members of our armed forces. Because of this, federal rules and regulations on cybersecurity continue to tighten.

The Department of Defense (DOD) enacted a set of strict cybersecurity and breach reporting regulations in August of last year following a string of cyberattacks on American businesses and government contracting agencies. One IRS hack exposed the personal financial information over 700,000 U.S. taxpayers. In June of last year, hackers accessed the databases of the Office of Personnel Management, exposing SF-86 questionnaire data that military intelligence officers use to get top secret clearance. The breach disclosed names, addresses, social security numbers, financial data, and other personal information.

The Defense Federal Acquisition Regulation Supplement (DFRAS) cybersecurity rule, titled Safeguarding Covered Defense Information and Cyber Incident Reporting, requires that those participating in any kind of defense department contract (1) have security measures in place on all computer systems, and (2) report all incidents of cyber hacking or security breaches to the Department of Justice within 72 hours of discovery.

Read More

Upcoming Events

CGP Fall Training Conference – November 17th. The Westin TysonsCorner, VA

Register

April 13 2017 B2G Conference & Expo Joint Base Langley / Eustice

More Info

Watch out for GSA Events in 2017:

MARCH 7-8, 2017 IFMIPS (51V, 03FAC) Industry Day Event
May 2017 the GSA Federal Acquisition Training Symposium penciled in for in Huntsville, Alabama, and
June 2017 the Professional Services Industry Day in Tacoma, Washington.

CONTACT

The Gormley Group
1990 M Street, NW
Suite 480
Washington, DC 20036
www.gormgroup.com
info@gormgroup.com

Compliance

Trade Agreements Act (TAA) Compliance

The Trade Agreements Act (TAA) is the enabling statute that implements numerous multilateral and bilateral international trade agreements and other trade initiatives. The TAA applies to all GSA Schedule contracts. The TAA limits the country of origin for products sold through your schedule contract, in general, this means the following may be sold:

1. Articles that are wholly the growth, product, or manufacture of the U.S. or a designated country, or
2. Articles that are "substantially transformed" in the U.S. or a designated country into a new and different article of commerce with a name, character, or use distinct from that of the article or articles from which it was transformed.

For services, country of origin is determined by the country in which firm providing the services is established. Please refer to the TAA clause in your contract for complete details, including relevant definitions and the list of designated countries.

Remember that it is the responsibility of each Schedule vendor to ensure that product information is accurately incorporated into the contract and displayed on GSA Advantage!® throughout the life of the contract. It is a good practice to periodically review the country of origin of products offered on your GSA contract, as manufacturers sometimes change their manufacturing points. If you determine that a product country or origin has changed, the following directions can assist you in updating GSA Advantage!

For contractors not eligible for FPT:

- For products that are no longer TAA compliant, submit a modification request to delete the product from your contract and submit a revised pricelist via SIP or EDI,
- For products that list an inaccurate country of origin but are TAA compliant, submit a revised pricelist via SIP or EDI with the correct country of origin.

For contractors eligible for FPT:

- For products that are no longer TAA compliant, submit a “Deletions - Delete Product(s)” modification request to delete the product from your contract and your GSA Advantage! listing will be automatically updated.
- For products that list an inaccurate country of origin but are TAA compliant, submit a “Catalog Pricing” modification update your GSA Advantage! listing.

If you have any questions please contact your TGG Consultant