SPOTLIGHT

Brian Ralston, President, GA-Commonwealth Computer Research, Inc.

Brian Ralston is the President of GA-Commonwealth Computer Research, Inc. (GA-CCRi). He is a retired Air Force Colonel with 25 years of military experience in a wide range of analytic leadership roles.

Colonel Ralston previously led test and evaluation activities for the B-1B, KC-135, and Joint Strike Fighter platforms, conducted personnel analysis studies for the Secretary of the Air Force, served as the lead analyst for the Air Force A-1 staff, was an Assistant Professor in the Department of Mathematical Science at the United States Air Force Academy, and led program and budget analysis for the Office of the Secretary of Defense. In his final active-duty assignment, Colonel Ralston served as the Director of the Office of Enterprise Analysis at the National Reconnaissance Office (NRO) where he led an organization of more than 150 military, civilian, and contractor personnel to conduct analytic trade and performance studies, driving system and architecture decisions for the future $60B+ NRO enterprise.

Upon retirement, he directed the THRESHER program at CCRi, leading a team of 60+ software engineers, data scientists, computer engineers, and user experience specialists to deliver an air and maritime global situational awareness application for thousands of users across the Department of Defense (DoD) and Intelligence Community.

> **"The inclusion of CCRi within the GA group will accelerate the delivery of actionable intelligence through the dynamic conversion of data to knowledge."** said Neal Blue, CEO, GA President and Chairman. **"CCRi will continue to serve defense and intelligence communities while contributing to GA systems and strategic objectives."**

Prior to being selected President of GA-CCRi, Colonel Ralston was the Director for Modeling and Simulation at L3Harris Space and Airborne Systems, where he was charged with leading a team of 80+ engineers and analysts to develop a mission-level modeling and simulation capability to integrate analytic support across the company, drive technology development and corporate strategy.

Colonel Ralston is a graduate of the United States Air Force Academy with a B.S. in Operations Research. He also earned a M.S. degree in Operations Research from the Air Force Institute of Technology, and a Ph.D. from the University of Virginia in Systems and Information Engineering.

Welcome Colonel Ralston and CCRi!

WELCOME

On April 2, 2021, General Atomics (GA) announced the acquisition of Commonwealth Computer Research, Inc. (CCRi). CCRi is a leader in software engineering and data analytics for delivering real time, global situational awareness to government and commercial customers.

Our Spotlight this Issue:

Please join us in welcoming Colonel Ralston and CCRi to the GA family!

SUPPLIER FOCUS

Supplier Performance Award Winner Supports GA Through the COVID-19 Pandemic

In March of 2020, the world became a drastically different place. Overnight, millions of jobs were suddenly up in the air, as the world transitioned to a virtual work environment and took shelter from a historic pandemic. The food industry, as with many service-based jobs, was hit especially hard due to the nature of their work. **Eurest Culin-Art**, GA's top culinary supplier and two-time Supplier Performance Award winner, rose to the challenge of serving our GA locations, even in the face of uncertainty.

Ruth Carrillo, Food Services Director of Eurest Culin-Art at the GA Torrey Pines campus said the beginning of the pandemic was a "really hard time to work." In the span of about a week, the majority of on-campus employees grabbed the essentials from their offices and transitioned to remote work. This left the Eurest Culin-Art staff's immediate future in question. "I went home and told my husband that I didn't know if I would have a job anymore," Mrs. Carrillo said. "Everyone was confused about what would happen and feared getting sick themselves" added **Ignacio "Manny" Ortiz**, Chef for Eurest Culin-Art at GA Torrey Pines.

Eurest Culin-Art staff, left to right: Director Ruth Carrillo, Erik Blue, Cesar Cazares, Katrina Aguirre, Karen Gibson, Lizeth De Haro, Jose Aguyo, Ana Estrada, Chef Manny Ortiz.

To their delight, GA kept all cafeterias open, implementing strict protocols according to Centers for Disease Control and Prevention (CDC) guidelines to keep everyone safe. The staff received hours of training on enhanced cleaning practices, utilization of Personal Protective Equipment (PPE), and methods to use if guests did not adhere to guidelines. Staff met daily to be briefed on any new developments.

Graciously, GA leadership made the decision to provide free ready-made meals for on-campus employees during the first few months of the pandemic. The meals were placed in the hot bar for "grab and go," minimizing in-person interactions. At first, with such a quiet campus, it was unknown whether this program would benefit employees. On the first day, 400 on-campus employees showed up for lunch. They were greeted with the same warmth as before, even if service looked a bit different.

Supplier Performance Award Winner Supports GA Through the COVID-19 Pandemic

At first, with such a quiet campus, it was Staff would smile and wave as critical onsite employees grabbed their lunch. "After the first week, everything felt safer because I knew we were doing everything we could to protect people in our space," Mr. Ortiz said. "We all have families to go home to and it's our job to protect not only our families, but the families of our guests as well."

Both Mrs. Carrillo and Mr. Ortiz discussed food shortages and supply chain disruptions. "We did an inventory of everything we had and then made menus based on what we knew we could provide," Mrs. Carrillo said. "To this day, there are still some items we are unable to get," Mr. Ortiz said. When supplies were available, strict inspections were done to ensure the food was safe for consumption. In the kitchen, items were wiped down before they were put away. "We didn't know how the virus travelled at that time, so we took every step possible to ensure the food was safe," Mr. Ortiz said.

More recently, as our GA headquarters has fully reopened, Ruth and Manny touched on some practices that will continue in a post-pandemic world. Practices like the intensive cleaning schedule, "grab and go" meals, and individually wrapped utensils are among some of these enhancements. "Happiness is related to food, and it's important that our dining area keeps people safe and makes them happy," Mrs. Carrillo said.

Ruth and Manny are thankful that GA provided the resources they needed to keep everyone safe and healthy.

"GA cares about their employees, first, and reacted to [the pandemic] differently than many other companies did. [GA employees] are truly the heart of the company," Mrs. Carrillo said.

"We never stopped working, and we are appreciative to GA for keeping everyone employed," said Mr. Ortiz. "GA is much more than just a company, it's a family."

GA thanks **Eurest Culin-Art** for their consistent efforts to keep us all safe and happy through the pandemic and as we fully return to on-campus operations.

FACT BOX

Why does GA require Supplier's to maintain a "Medium Assurance Certificate"?

In order to report cyber incidents when DFARS 252.204-7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting" applies, the Supplier shall have or acquire a Department of Defense (DoD)-approved medium assurance certificate to report cyber incidents.

DoD Medium Assurance certificates are issued under the DoD External Certificate Authority (ECA) program and are used to conduct business with the DoD and other government entities. This certificate is stored in your browser certificate store on your local PC or laptop.

For information on obtaining a DoD-approved medium assurance certificate, see https://public.cyber.mil/eca/.

COMPLIANCE CORNER

Improving your Department of Defense (DoD) Cyber Assessment Summary Score

As required by our Supplier Code of Conduct, Suppliers will take all appropriate measures to combat the increasing frequency of cyberattacks. They will implement the controls and processes necessary to safeguard information under their control while reporting and mitigating any compromise of systems or information. This responsibility includes performing the requisite assessments, specifically when required by DFARS 252.204-7020 "NIST SP 800-171 DoD Assessment Requirements" and working proactively to improve scores and overall cybersecurity postures. Read on to learn about how to manage and improve your score.

DFARS 252.204-7020 requires that all suppliers subject to the DFARS 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," have a current summary score ("current" means not more than three years old) posted to the DoD Supplier Performance Risk System (SPRS).

After conducting self-assessments in accordance with the DoD NIST SP 800-171 Assessment Methodology, some suppliers in the DoD supply chain realized that while they may have a System Security Plan (SSP), their summary scores didn't reach 110, a perfect score. Don't fret if this is you; there are important steps you can take to help strengthen your cybersecurity program and improve your summary score:

1. **Review and update any applicable Plan of Action and Milestones (POAM)** –

    Is your POAM current? Are the dates reflected in the POAM achievable? If your POAM dates are no longer accurate, it's time to re-baseline your schedule.

2. **Manage to your POAM** –

    Have you allocated the resources necessary to execute upon any POAM? Assign responsibility and hold your team accountable to execute according to the POAM. Proactive management of any POAM items can make or break your progress to becoming cyber secure.

3. **Leverage publicly available resources** –

    Are you using all the Government or industry resources available to you? A list of resources can be found on the GA website under Supplier Cybersecurity. New resources are added frequently so check back often. Check out "Project Spectrum", a DoD resource.

4. **Hire a professional** –

    Would an outside professional help you to assess and move forward? The NIST SP 800-171 was written for cybersecurity professionals. If your company does not have the required expertise in-house, contract the services of a cybersecurity professional or company with experience in supporting organizations. A quick web search will turn up providers you can begin to vet and engage.

5. **Keep your Summary Assessment Score up-to date** –

    Have you improved your score? Don't forget to update your score in the DoD SPRS and with GA, using the Ariba Certification of Compliance with DoD Cybersecurity Assessment Requirements. Contact your Purchasing Representative for any assistance.

    The full text of the interim rule can be found here.

These clauses will apply to most entities in the Defense Industrial Base, including Suppliers to GA who handle Federal Contract Information (FCI) as defined in FAR 52.204-21, "Basic Safeguarding of Covered Contractor Information Systems," Controlled Unclassified Information (CUI) and Covered Defense Information (CDI) as defined in DFARS 252.204-7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting."

If these clauses will apply to work you do with GA you will soon receive an invite in Ariba® to complete new representations and certifications. Please review the rules as soon as practicable and undertake necessary actions.
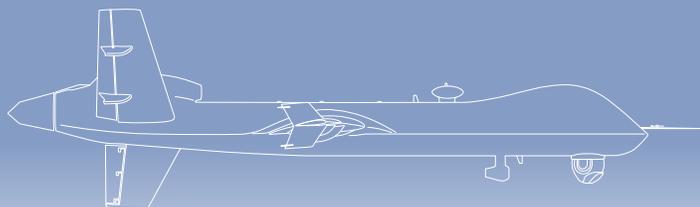
On The Horizon
The Supplier Performance Program is on a Trajectory for Expansion

In both the Winter 2019 and Fall 2020 Supplier Newsletters we profiled GA's Supplier Performance Program (SPP), with an overview of the SPP's purpose, it's various performance metrics, and the anticipated transition to an improved system platform.

GA is excited to announce that the enhanced platform was successfully launched April, 2021 and the transition is complete. Suppliers currently engaged with SPP operations now receive updated Performance Scorecards that reflect the improved and industry-benchmarked performance metrics. Furthermore, these metrics align with GA Aeronautical Systems, Inc. (GA-ASI) which streamlines feedback for Suppliers that support both GA organizations.

Immediate benefits to this transition include the use of intuitive and straightforward metric calculations, as well the ability to rapidly increase Supplier membership. To that end, April's launch enabled a 28% growth in participants, with a goal of further expansion in coming months.

Since its inception in 2008, SPP has continued to evolve and assist GA Purchasing Representatives by providing crucial data to assess performance capabilities, and acting as a key input to awards and recognition. This transition aligns with GA's constant focus on continuous improvement.

Did you miss GA at the 2021 Navy Gold Coast event?

GA is a Silver sponsor this year and our next Supplier Newsletter will have a wrap-up of the virtual event and our participation in it.
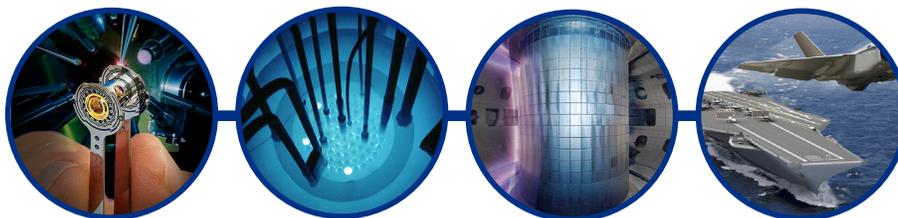
QUALITY MATTERS
Avoiding the Costs of Counterfeit Parts

GA relies upon its suppliers to comply with all regulatory requirements, quality standards, and best practices regarding counterfeit avoidance, detection, and reporting. Counterfeit parts have become a multi-billion-dollar industry. Technological advancements and an increasingly global supply chain have made the threat of counterfeit parts even more likely.

The threat is real, and some of the costs are immeasurable.

A federal regulation we'd like to highlight is FAR 52.246-26, "Reporting Nonconforming Products" (JUN 2020). This FAR clause requires government contractors and subcontractors to report nonconforming items, including those suspected to be counterfeit, to the Government-Industry Data Exchange Program (GIDEP) at www.gidep.org. GIDEP is operated cooperatively between government and industry, and according to its website has the aim "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." GIDEP membership is free.

Reporting to GIDEP is an important element of counterfeit part avoidance within the government contracting industry. Now more than ever, companies should focus on proactive counterfeit avoidance, as opposed to just detection. Being an active member in GIDEP, whether required by contract or not, provides you access to other industry reports, and critical technical data, which can help you to avoid a counterfeit issue before it materializes. Detection can be too late to avoid costly impacts, like schedule delays and loss of reputation.

The serious nature of such risks prompted the need for tighter regulations and quality standards regarding counterfeit avoidance in government procurements. While these may seem cumbersome, they serve to protect the U.S. and the world at large. Embedded in them are best practices that apply to all industries — including, maintaining a robust Approved Supplier List, implementing a counterfeit avoidance and detection program, and procuring parts from authorized Original Equipment Manufacturer (OEM) distributors whenever possible.

Thank you for your efforts to avoid these costs and to help GA deliver safe and reliable products.

FACT BOX
What are counterfeit parts?

The Federal Acquisition Regulation (FAR) defines them as "parts that have been unlawfully reproduced or altered and misrepresented to be authentic." Legal issues aside, these parts often fail required product specification and testing. When undetected, these defective parts can pose significant safety risk to the end user, including loss of life — a cost too great to bear. To GA and its customers, defective parts are also a threat to national security and the critical national infrastructure our products serve.