COVID-19 Alert: The health, safety and well-being of our employees, customers, community and Suppliers are our top priorities as we provide continued support and service to our US government and non-government customers. We are closely monitoring the COVID-19 situation and advising employees and stakeholders to take necessary precautions. Please visit **www.ga.com** and click 'Procurement' or 'Visitor Information' for announcements and additional information.

SupplierNewsletter

GENERAL ATOMICS

Fall 2020

SPOTLIGHT

GA Supplier Day Goes Virtual!

In spite of global challenges, General Atomics (GA) has continued to live up to its mission of 'Global Progress Through Technology.' Your support has been instrumental to our success. In celebration of your contributions, GA will hold its 2020 Supplier Day on November 17, 2020. This event will be packed with opportunities to meet our Buyers and subject matter experts (SMEs), hear from keynote speakers and look for ways to grow and enhance your relationship with GA. To adapt to these changing times, our 2020 event will be **virtual**.

A virtual event means that we can harness the power of technology and offer multiple rounds of concurrent sessions focused on topics that matter to you, such as cybersecurity, critical quality requirements and upcoming tool enhancements to support our working relationship with you. It also means we are able to invite more of you.

In addition to learning and networking, GA will recognize specially selected Suppliers who have made the most significant contributions since our last Supplier Day. So far, in addition to the awards ceremony, we've confirmed that Mr. Scott Forney, the President of GA Electromagnetic Systems (EMS), will join us along with other distinguished GA Executives.

If you are an active GA Supplier and did not already receive an invite, please see our Save the Date or email us at SupplierEngagement@ga.com.

INTRODUCTION

Following the end of our U.S. Government (USG) customer's fiscal year, we celebrate the accomplishments of our customers, employees and Suppliers. We recently wrapped up our 'Silver' level sponsorship at the Department of the Navy Gold Coast 2020 and are now preparing for own upcoming Supplier Day.

QUALITY MATTERS

Roll-out of Quality Assurance Resources Through 2021

Part of our Quality Policy is to continually improve our products and process through coordination with our suppliers. That includes providing you with resources to help you understand and comply with our Quality Assurance (QA) requirements.

Some of you may recall our previous QA awareness material and noticed it is no longer available on our website. That's because we've been working to update and improve it so it's easier to find the topics you need. Instead of one large comprehensive guide, we plan to roll out topical modules in the coming months. This way, you can search for specific topics and pinpoint issues affecting your QA program quickly and easily.

Our first modules on "Welding and Brazing Requirements" and "Raw Materials and Metals Requirements" will be presented during our 2020 Supplier Day. This will soon be followed by additional modules added to our website over the coming year. Remember to contact your GA Authorized Purchasing Representative for any questions specific to your GA Order.

COMPLIANCE CORNER

Representations and Prohibitions Regarding Telecommunications Acquisitions, Part II

As discussed in our last 'Compliance Corner,' the U.S. Government (USG) continues to focus on cyber threats to information and product integrity. To that end, section 889 of the National Defense Authorization Act (NDAA) for fiscal year (FY) 2019 (Public Law 115-232- Aug. 13, 2020) introduced new regulations under a phased implementation referred to as Part A and Part B.

Part A, effective August 2019, prohibited Contractors from **providing** to the USG "any equipment, system or service that uses covered telecommunications equipment or service as a substantial or essential component of any system, or as critical technology as part of any system."

Part B, which became effective August 13, 2020, expands the prohibitions beyond work performance under government contracts. More specifically, Part B precludes the USG from entering into a contract, or extending or renewing a contract, with any entity that **uses** "covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system," regardless of whether such equipment, system or service is used for military or commercial (non-government) applications.

For more information, please see the General Services Administration guidance on Section 889 here.

All GA Suppliers must be familiar with and, adhere to the requirements of Section 889 of the NDAA. Please review your proposals prior to submission, (continued on page 2)

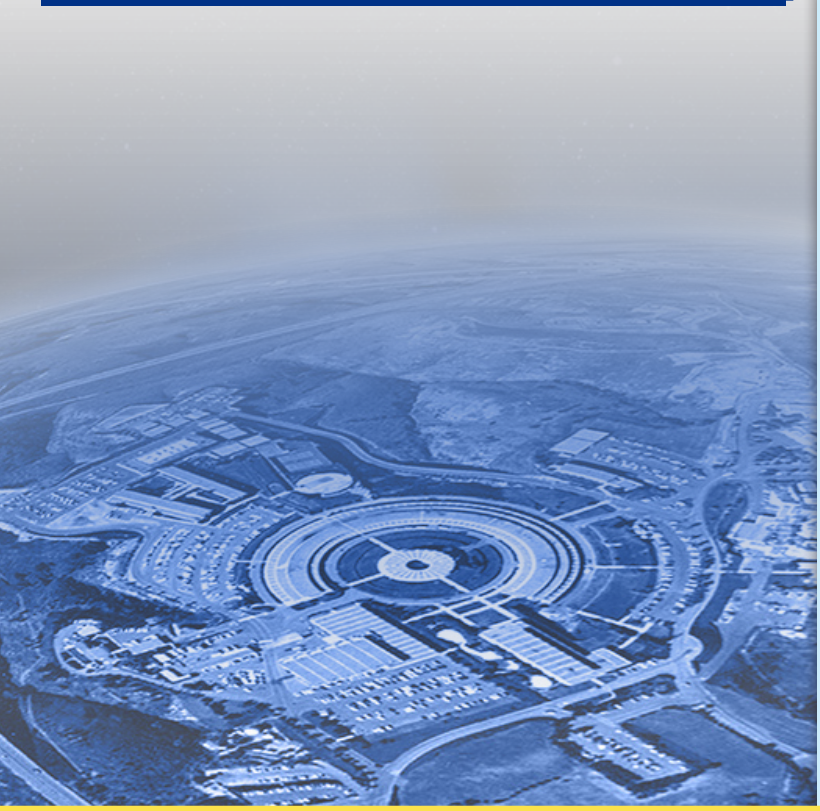
ON THE HORIZON

Launching the Enhanced Supplier Performance Program

In our first Supplier Newsletter we briefly profiled the Supplier Performance Program (SPP) and its comprehensive performance metrics platform. While originally scheduled for a mid-2020 launch, we recognize that the current COVID-19 situation has understandably impacted much of our supply base and associated operations and adjusted our timeline accordingly. With our sights on the upcoming 2020 Supplier Day, we have elected to shift our launch and seize the opportunity to speak directly with our suppliers and introduce them to our enhanced SPP.

While many suppliers are currently engaged with SPP and regularly receive performance feedback from GA, this new platform will enable us to greatly expand supplier membership; in the coming weeks, many of you will receive communications soliciting your performance contacts, to ensure these vital metrics and scorecards are received by the appropriate personnel. The enhanced SPP platform will continue providing crucial data to assess performance capabilities and will act as a key determinant in our decision-making.

Don't forget to reserve your spot at the 2020 Supplier Day! RSVPs are accepted until October 30th, 2020 at SupplierEngagement@ga.com.



COMPLIANCE CORNER

(continued from page 1)

and any open Orders, and inform your Purchasing Representative of concerns regarding your compliance. Note that GA may ask for representations to demonstrate your understanding and compliance with Section 889. For example, you may be asked to represent whether your company will provide or use "covered telecommunications equipment or services," as defined in Section 889 of the NDAA.

Please visit GA Procurement for this and other regulatory updates.

Safeguarding of Information & Cybersecurity

Is your System Security Plan adequate?

Protecting and securing critical industry information and responding vigilantly to cyber warfare threats requires implementing, documenting and managing the security controls for your information systems in a System Security Plan (SSP). SSPs have been an industry standard, and a requirement for the Defense Industrial Base and entities subject to the Defense Federal Acquisition Regulations Supplement (DFARS) 252.204-7012 since January 1, 2018.

The SSP is vital to demonstrate your compliance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171; and, for you or a customer to evaluate the security afforded by your information system. An effective SSP is continuously evaluated and updated to align with the latest standards and reflect changes to the organization.

Demonstrating compliance means more than simply stating it. To be adequate, the SSP will address each of the NIST SP 800-171 (current revision) controls by (1) documenting how each standard is met, (2) identifying the relevant policy, procedure or process that supports the standard, and (3) using examples of evidence to back it all up (i.e. logs and/or other applicable artifacts). Use NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information," which is composed of 320 Organizational Actions (OAs) that an SSP should address, to assess your organization.

The Department of Defense (DoD) and other customers may request your SSP for inspection. In fact, in late 2019, the DoD tasked the Defense Contract Management Agency (DCMA) with inspecting SSPs and other related cybersecurity compliance requirements. A key question this raises for many companies is "how can I produce an SSP I can share without divulging sensitive information about my networks that could lead to compromise?" The simple answer is to reference artifacts, but maintain any sensitive information external to the SSP. This way you are able to share your SSP with a customer while protecting sensitive information about your networks and processes.

Effective compliance with NIST 800-171 will prepare your organization for the upcoming implementation of the Cybersecurity Maturity Model Certification (CMMC). Please refer to GA's cybersecurity website for information including the latest DFARS Cybersecurity interim rules.

As a high technology and high concept provider of Defense and Energy solutions, GA is uniquely positioned for growth and success. Global progress through technology remains our mission. GA appreciates the support of its Suppliers in accomplishing this mission.

Remember to contact your Purchasing Representative about any questions regarding open Orders or your continued performance. Your Purchasing Representative is your primary point of contact.

Please advise your Purchasing Representative when contacted by other GA personnel.
If you have any comments or questions about this publication, please contact us at SupplierEngagement@GA.com.