GENERAL DYNAMICS
NASSCO

Supply Chain Business Controls

Supply Chain Management
May 20, 2020

To: GD NASSCO Suppliers

Subject: Social Engineering, Scams, and Fraud Awareness

Dear Supplier:

To protect your business from losing product and revenue, particularly with the new dependency on remote work locations, please consider such warnings as those identified by the Cybersecurity & Infrastructure Security Agency whenever your employees receive on-line requests. For more information on COVID-19 warnings about scams and frauds and prevention tips, please visit the "Scams and Fraud" section of https://www.usa.gov/coronavirus. These protective measures include the follow actions as you review requests:

1. Consider faxed documents and/or an insistence to communicate by fax suspicious
2. Independently obtain the office phone number for the official contact and call them directly to confirm legitimacy
3. Send a new email to the person using the email address that you know is legitimate, instead of simply hitting reply
4. Look for suspicious shipping or banking points of contact and locations. Independently confirm the legitimacy of the address and points of contact
5. Check for misspellings or wrong domains within links, email addresses, and content
6. Check for unusual language not typical of native English speakers
7. Check for distorted seals and graphics
8. If the request is for something outside your specialty, it may be fraudulent.

Please report suspected criminal activity and fraudulent schemes to related to the COVID-19 pandemic to COVID19Fraud@dhs.gov.

If you have any questions/concerns, reach out to the following individuals:

NASSCO Business Controls
Business.Controls@nassco.com

Suzanne Trinh, Supply Chain Professional
(619) 544-8888 x 5164/ Suzanne.Trinh@nassco.com

Valerie Fusco, Manager SCM
(619) 544-8462 / valerie.fusco@nassco.com

Thank you for your support.

NASSCO Supply Chain Management Team