

**April 17, 2024**

## **Awareness of Northrop Grumman Employee Impersonation**

---

Dear Valued Northrop Grumman (NG) Supplier,

Please be aware that NG is receiving multiple complaints of a fraudulent actor impersonating affiliation with NG and engaging suppliers with false procurement requests or other paperwork. This may be an attempt to conduct financially motivated fraud or an attempt to deliver malware and appears to be part of a much wider fraud campaign targeting and spoofing the identities of multiple companies. NG only uses the domain "northropgrumman.com" for our websites and "ngc.com" for email transactions. NG also recommends restricting the ability to change delivery addresses when fulfilling procurement requests.

Please report any suspicious activity/emails to Northrop Grumman's Cyber Security Operations Center (CSOC) at [csoc@ngc.com](mailto:csoc@ngc.com) or (877) 615-3535.

Please continue to utilize the Northrop Grumman [Cybersecurity Resources for Suppliers](#) as well as the [CyberAssist](#) website to access helpful information and resources.

Our suppliers are essential to Northrop Grumman meeting our program commitments to our customers. Partnering and sharing best practices better prepares us to mitigate cybersecurity threats and strengthens our collective information security posture across the entire Defense Industrial Base (DIB). Thank you for your continuous support and continued commitment to enhance your company's cybersecurity position.