



Supplier Announcement

Critical Alert: SolarWinds Compromise

December 2020

Valued General Atomic Aeronautical Supplier,

As expressed in our Supplier Code of Conduct, General Atomic (GA) is committed to protecting and securing sensitive information and responding to the growing cyber threat posed to our customers and industry. As a Supplier to GA, you share in this commitment. Please read on regarding the recent global intrusion campaign that leveraged SolarWinds Orion® to compromise public and private organizations.

SolarWinds was the victim of a cyberattack which inserted malware (SUNBURST) into their Orion business software update platform. On December 13, 2020, FireEye uncovered the campaign leveraging Orion to distribute the malware to customers of SolarWinds. On December 14, 2020 news reports began surfacing about widespread compromise of Government and contractor systems that use SolarWinds Orion.

In response, the Cybersecurity & Infrastructure Security Agency (CISA) issued Emergency Directive 21-01, "[Mitigate SolarWinds Orion Code Compromise](#)". CISA most recently updated Emergency Directive (ED) 21-01 on January 6, 2021 to "[Supplemental Guidance version 3: Mitigate SolarWinds Orion Code Compromise](#)", providing guidance that supersedes Required Action 4 of ED 21-01 and Supplemental Guidance versions 1 and 2.

Details of the attack continue to evolve and all companies that use SolarWinds Orion are strongly encouraged to follow and implement the guidance from CISA. Defense Industrial Base (DIB) Suppliers with access to the DIBNet portal received numerous communications, including Alert 21-007, from The Defense Cyber Crime Center (DC3).

Please review any contractual obligations, specifically those including DFARS 252.204-7012, to determine whether a cyber incident report to DC3 at <https://dibnet.dod.mil> is required. If you find it is necessary to file a report with DC3, please remember to inform your GA Purchasing Representative of the report number.

Additional information can be found on our Procurement Cybersecurity website at <https://www.ga-asi.com/suppliers/cybersecurity>.

Note: The information herein is provided for informational purposes only and does not constitute legal advice; nor does it imply a change in any existing Order.