CYBERSECURITY

Are you interested in becoming a Department of Defense Contractor?

All Department of Defense (DoD), General Services Administration (GSA), and NASA contractors must have met the Federal Acquisition Regulations (FAR) minimum cybersecurity standards as of December 31, 2017. On November 30, 2020, a second significant DoD cybersecurity contracting requirement became effective with three new Defense Federal Acquisition Regulation Supplement (DFARs) clauses. If you are not compliant, your company is at risk of not obtaining or even losing federal contracts.

If you're like many manufacturers, you may not know everything that is expected or even how to get started. To make this process easier, Purdue MEP has assembled a team of cybersecurity experts to help ensure you are compliant with these new standards.

Our experienced team has designed a comprehensive four-step cybersecurity program. This is intended to help you gauge your current situation, then tailor a plan specifically for your company's internal capabilities, budget, and time sensitivity.

Four-Step Cybersecurity Program

- **Step 1: Discovery** – an assessment of your company's practices related to the new standard. If necessary, a gap analysis will be completed to document the scope to be remediated.
- **Step 2: Remediate to Meet New Standard** – supports all fixes necessary for compliance. Sample work could include updating firewalls, patches, policy development, employee training, physical security, network configuration, etc.
- **Step 3: Test and Validate** – verifies all technology and physical security aspects are working properly.
- **Step 4: Monitoring/Reporting** – establishes ongoing monitoring and scanning of the required enterprise network. Creates a working process to log, remediate, and report (as required) cyberattacks.

DID YOU KNOW?

- 61% of experts in technology and policy predict a major cyberattack causing widespread harm will occur by 2025, according to a Pew Research Center report.
- $445 billion is lost annually to cybercrime and espionage across the entire world economy, according to the Center for Strategic and International Studies.
- 46,605 breaches of federal computer networks occurred in 2013 according to the U.S. Computer Emergency Readiness Team.

Don't risk being unprepared. Contact us today to see how we can help!