PennState
Applied Research Laboratory

SUPPLY CHAIN
724-430-4203
SUPPLIERRELATIONS@ARL.PSU.EDU
JANUARY 2023, VOL 2

# LET'S WELCOME IN 2023!

ARL has a strong commitment from our sponsors and is currently ramping up a large procurement activity. We welcome your feedback and invite you to email SupplierRelations@arl.psu.edu with suggested topics or areas of interest.

We appreciate your partnership as you play a vital role in helping ARL and our sponsors achieve our collective mission.

## MORE ABOUT ARL

ARL is a DoD-designated University Affiliated Research Center (UARC). ARL has core competencies in: Undersea Systems, Fluid Dynamics and Acoustics, Communications, Information, and Navigation, and Materials and Manufacturing.

**What is ARL's mission and how is it funded?**

ARL receives mission-based sponsorship from the US armed forces, government agencies, and industry. These sponsors define the mission and collaborate with ARL to leverage ARL's core competencies in projecting best solution(s). Missions routinely involve development of mechanical and electrical hardware and other technologies. ARL has some internal capabilities – but relies heavily on suppliers for most hardware. Development typically includes proof of concept, prototyping, and occasionally Low Rate Initial Production (LRIP). ARL designs, including supply chain details, are typically provided to the sponsor. As a result of your participation with ARL, your company may be called to provide parts for full production!

## SECURITY Q & A: THREAT ACTORS

A threat actor is a person or group that performs malicious acts to cause harm to the cyber realm, including computers, other devices (phones), networks, organization computing systems.

- Nation States – Spies stealing defense/industry secrets
- Criminals - use phishing to steal bank logins - money
- Insiders - steal intellectual property – money, revenge
- Hacktivists - use digital means for political agenda
- Hobbyists - compromise networks - because they can.

Threat actors target small organizations that supply a larger one. Most threat actors goal is to steal as many login credentials as possible no matter what industry you're in.

**What can I do?** Create long, strong passwords for all accounts, update the applications and software on your devices, and learn about phishing - the #1 way threat actors steal login information.

## EVOLVING COMPLIANCE REQUIREMENT

**What is CMMC?**

Cybersecurity Maturity Model Certification (CMMC) is a future DoD certification that aligns government cybersecurity standards and puts a strong focus on NIST 800-171a. CMMC consists of three levels of certification.

**Why should I care about CMMC?**

CMMC is expected to start to be included in DoD contracts beginning mid-2023. If you do not have CMMC at the required level, you will not be able to exchange CUI with organizations like ARL, which translates into loss of business.

**Is there help available to understand and deal with CMMC?**

**Yes.** The Air Force provides a FREE service to Small Businesses in the Defense Industrial Base through a government-funded program called Blue Cyber. Blue Cyber offers advice and cybersecurity resources through seminars, resources, presentations/videos, and a call center (with live people!). Blue Cyber also provides advice on implementation and assessments of NIST800-171a, along with help for your companies System Security Plan. To learn more, visit:

https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/


*Current and projected CMMC evolutionary timeline*

We understand evolving compliance may place additional burden on your business. We appreciate your willingness to continue to meet DoD security requirements.