PennState
Applied Research Laboratory

SUPPLY CHAIN
724-430-4203
SUPPLIERRELATIONS@ARL.PSU.EDU
2023, VOL 3

ARL continues to receive strong support from our sponsors and several current programs have major procurements in process. We want your feedback and invite you to email SupplierRelations@arl.psu.edu with any questions, 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.

SECURITY

Did you know that more than 4 out of 5 Defense Industrial Base (DIB) contractors have experienced a cyber-related incident? Cyber Related incidents jeopardize the confidentiality, integrity, and availability of digital information systems (www.dhs.gov).

What can you do to prevent a cyber-incident?

- Mobile Devices: Keep company information to a minimum on your device. Lost device = lost data, including company data, emails, texts, and photos (and all your personal data!).
- Unauthorized/non-company devices: Don't plug in unauthorized devices such as old flash drives, etc. Give it to your IT department. They should open the device on a standalone computer that won't impact your network.
- Passwords: Password complexity is a must. Don't share your passwords and don't use the same passwords.
- Email Use: Don't use your work email for personal reasons and vice versa.
- Unauthorized activity: Activities such as music streaming, movie streaming, and pirated software can result in the download of malware.
- Phishing: If something is too good to be true, it probably is. Malicious emails often phish for usernames, passwords, credit card numbers or money.
- Social Engineering: Different techniques attempt to convince you into revealing specific information.

MORE ABOUT ARL

After the end of WWII, the US military started investing heavily in higher education nationwide. At the same time, Harvard terminated its Underwater Sound Laboratory (USL); consequently Penn State hired Eric Walker, USL's assistant director to head its electrical engineering department, and the Navy transferred USL's torpedo division to Penn State - where it became the Ordnance Research Laboratory (ORL), which eventually became the Applied Research Laboratory.

BACK TO BASICS - WHAT IS CUI?

Controlled Unclassified Information (CUI) is information that is not classified, but requires additional protective measures. CUI is a range of information such as personal information, proprietary information, or information considered critical to national security including Controlled Technical Information (CTI), and with items under Distribution Statements B through F or Export Controlled data (including ITAR)

Why is it important?

Because there are fewer controls over CUI as compared to classified information, CUI is the path of least resistance for adversaries. Loss of aggregated CUI is the one of the most significant risks to national security, directly affecting safety and lethality of our war-fighters.

Your responsibility!

As an organization that may receive CUI/CTI, it is your responsibility to ensure that your systems, personnel and processes protect the information according to NIST 800-171. You must also obtain a Supplier Performance Risk System (SPRS) score and maintain Joint Certification Program (JCP) certification. In 2023, the Department of Defense is expected to finalize the rule making process for the new DFARS clause 252.204-7021. As a result, companies will be required to maintain a Cybersecurity Maturity Model Certification (CMMC).

Supplier Performance Risk System | (disa.mil)

252.204-7021 CybersecurityMaturity Model Certification Requirements. | Acquisition.GOV

If your company needs assistance with understanding your responsibilities related to CUI, NIST 800-171a or any ARL work, please reach out, there are free resources to help.

Even the smallest of pieces are important to the big picture!

If your company has questions about the Cybersecurity requirements or aren't sure how to implement them, the Blue Cyber Program is a free resource available to small business contractors.
https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/