DoD Cyber Security Requirements

Small businesses are increasingly common targets for cyber-attacks. DoD SBIR requires small businesses to follow the Federal Communications Commission (FCC) guidelines for a cybersecurity plan. The NIST 800-171 standards apply if the SBIR effort involves Controlled Unclassified Information (CUI). Under DFARS § 252.204-7012-Safeguarding Covered Defense Information and Cyber Incident Reporting, DoD contractors must comply with two basic cybersecurity requirements:

1) Provide adequate security to safeguard covered defense information that resides in or transits through their internal unclassified information systems from unauthorized access and disclosure; and 2) Rapidly report cyber incidents and cooperate with DoD to respond to these security incidents.

The Small Business Association (SBA) recommends the following best practices:

Safe internet practices

- Do not surf the web with an administrative account.
- Do not download software from unknown pages.
- Do not download files from unknown sources.
- Do not respond to popup windows requesting you to download drivers.
- Do not allow any websites to install software on your computer.
- Protect passwords, credit card numbers, and private information in web browsers, and conduct online business and banking on secure connections.

Safe email practices

- Do not open email attachment if you do not recognize the sender.
- Do not reply to unsolicited emails.
- Do not click on links in an email unless it is from a trusted source.

Safe desktop

- Limit employee access to data and information and limit authority to install software.
- Use separate computer accounts for each user.
- Use passwords and do not share.
- Create strong passwords – no names, birthdates, or personal information – and change every three to six months.
- Use screen locking, log on and off, and power down your system at the end of the day.
- Don not put "lost" infected USB drives into systems.
- Consider encrypting sensitive data on your system. Use encryption tools that will work within your computing environment.

Safe network

- Install anti-virus software, company-wide detection tools, and use up-to-date definitions to protect against viruses, Trojan horses, and malware.
- Use firewalls to limit access, and update operating systems and applications with the latest patches.
- Routinely backup your data to prevent against catastrophic loss.

References

DoD OSBP Cyber Resources: https://business.defense.gov/Programs/Cyber-Security-Resources/
Center for Development of Security Excellence: https://www.cdse.edu/Training/Toolkits/Cybersecurity-Toolkit/#trainingawareness
SBA Cybersecurity Business Guide: https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats;
Federal Communications Commission (FCC) guidelines: https://www.fcc.gov/general/cybersecurity-small-business