CYBERSECURITY- issues and actions

Imagine that you are piloting a state of the art fighter jet on a night mission. In just a few minutes you will be feet dry – back over land and based upon updated navigation information will make one more course correction to the target. Once again, you are flying into hostile territory as you have done many times before.

Tonight there is no moon; it is inky black. The only light is a dim glow from the digital instrument panel. You feel confident in the superiority of your technology – your communications, weapons, navigation and electronics.

But what if your adversary could listen in on all of your conversations, and their aircraft and missiles had all the same capabilities as yours? Whether the technical data that your adversary used to improve his platforms was mishandled, stolen or hacked, the aircraft you are piloting no longer has a tactical advantage.

Ultimately it is our national intellectual property - the engineering, the science and all of the advances - that protects members of our armed forces and keeps the country safe. Everyone who has access to intellectual property must do their part to safeguard this information. In the performance of contracts the very intellectual property that keeps us safe is entrusted to members of the vendor community to use in the manufacture of goods and services.

Proper handling and storing of this information is critical. As a vendor, you must comply with the rules and regulations that govern the information the government shares with you.

The following are some steps that will assist you in ensuring you comply:

1. Determine if data (information) has any special handling requirements
2. Unclassified contracts may still have rigorous information handling requirements
3. Know the handling requirements for any contract data
4. Develop an IT security plan and processes IAW with NIST Special Publication 800-53
5. Always use anti-virus software and keep definitions current
6. Only use portable media from trusted sources, even then scan
7. Review and incorporate Federal Acquisition Regulations (FAR), Department of Defense FAR supplement and/or other requirements into your security plan
8. Train all team members who will require access and use the data
9. Review eligibility of your IT service provider (external) and staff (internal – external)
10. Meet with suppliers to determine their eligibility, share requirements and train as needed
11. Monitor your network and report as required
12. Review and update your program, incorporate industry best-practices for security
13. Participate in online forums such as Infraguard or the Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Program
14. **Pay attention to the basics** – passwords, access lists, using email, don't assume all is well!

It's up to all of us to protect government intellectual property!

Wisconsin Procurement Institute – Wausau Office
Marc N. Violante, Director, Federal Market Strategies, email: marcv@wispro.org, phone: 920-456-9990

CYBERSECURITY- resources and links

National Initiative for Cyber Security Careers and Studies: https://niccs.us-cert.gov/

Homeland Security, Cybersecurity Publications: http://www.dhs.gov/cybersecurity-publications

Defense Industrial Base Cyber Security: http://dibnet.dod.mil./

NIST Special Pub 800-53: http://dx.doi.org/10.6028/NIST.SP.800-53r4

DoD Center for Development of Security Excellence: http://train.cdse.edu/

FCC Small Biz Cyber Planner 2.0: https://www.fcc.gov/cyberplanner

SBA Cyber Security information: https://www.sba.gov/navigation-structure/cybersecurity

Federal Acquisition Regulations: https://www.acquisition.gov/?q=browsefar

Department of Defense Federal Acquisition Regulations Supplement:
http://www.acq.osd.mil/dpap/dars/dfarspgi/current/

InfraGard is a partnership between the FBI and the private sector: https://www.infragard.org/

Credible source for security information: http://krebsonsecurity.com/

DoD Instruction 5230.24 – Controlled Technical Information (Distribution Statements)

DFAR 252.204-7000 – Disclosure of Information

DFAR 252.204-7302 - Safeguarding unclassified controlled technical information

Programs with requirements for handling information

a. Joint Certification Program (JCP) – US- Canada
b. Nuclear Regulatory Commission
c. Missile Technology Export Controls
d. Export Administration Regulations (EAR)
e. Arms Export Control Act – International Traffic in Arms Regulations