Cybersecurity is critical to all businesses, especially small businesses. Continuing from our previous section, Cybersecurity Plans & Implementation for Small Business, next we cover cybersecurity standards related to government contracting, particularly defense contracting, though these standards are applicable regardless of whether or not you are seeking to become a government contractor, as they are comprehensive. Special thanks to the Center for Infrastructure & Security Assurance for their guidance on this topic.

Government Contracting Cybersecurity Standards

The Department of Defense (DoD) requires small business contractors to comply with their cybersecurity standards for the protection of unclassified data. These requirements are outlined through several regulations, covered comprehensively by the DoD (Protecting Unclassified Information) and summarized below for your convenience:

Defense Federal Acquisition Regulation Supplement (DFARS)

The **Defense Federal Acquisition Regulation Supplement Part 252** "*Solicitation Provisions and Contact Clauses*" (DFARS 252.204) governs cybersecurity requirements for federal contractors. It requires that contractors provide adequate security, report cyber incidents, submit any malicious software discovered and submit media to support damage assessment.

- Multi-factor authentication of local and network access
- FIPS-validated cryptography to protect CUI when transmitted or stored externally
- Develop a NIST SP 800-171 System Security Plan
- Possess External Certificate Authority (ECA) as verified by DCMA
- Report cyber incidents within 72 hours to DoD. Submit an incident report, any malicious software and provide access to information systems

DFARS further requires that contractors implement the **National Institute for Standards and Technology (NIST) Special Publication 800-171** "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" (NIST SP 800-171).

Access Control

- Limit information systems to authorized users
- Limit information system access to permitted transactions and functions

Awareness and Training

- Ensure manages, administrations and users are aware of policies, standards and procedures
- Ensure personnel are adequately trained to carry out assigned duties and responsibilities

Audit and Accountability

- Create, protect and retain information system audit records
- Ensure the actions of individual users can be uniquely traced to those users

Configuration Management

- Establish and maintain inventories of information systems (hardware, software, firmware)
- Enforce security configuration systems

Identification and Authentication

- Identify information users, process acting on behalf of users, or devices
- Authenticate (verify) the identities of those users, processes or devices prior to allowing access

Incident Response

- Establish an incident-handling capacity for detection, containment, recovery and user response
- Track, document and report incidents to appropriate officials and/or authorities

Maintenance

- Perform maintenance on organizational information systems
- Provide controls on the tools, techniques, mechanisms and personnel conducting maintenance

Media Protection

- Protect information system media containing CUI both paper and digital
- Limit access to CUI on information system media to authorized users
- Sanitize or destroy information system media containing CUI before disposal or release for reuse

Personnel Security

- Screen individuals prior to authorizing access to information systems containing CUI
- Ensure that CUI are protecting during and after termination and transfers

Physical Protection

- Limit physical access to information systems and equipment
- Protect and monitor the physical facility and support infrastructure for information systems

Risk Assessment

- Periodically assess the risk to operations, assets and individuals from information systems
- Periodically assess the risk associated with processing, storing or transmitting CUI

Security Assessment

- Periodically assess the security controls of information systems
- Implement a plan of action to correct deficiencies and reduce or eliminate vulnerabilities
- Monitor information system security controls on an ongoing basis

Systems and Communications Protection

- Monitor, control and protect communications at the internal and external boundaries
- Employ secure architectural designs, software development and systems engineering principles

System and Information Integrity

- Identify, report and correct information and system flaws in a timely manner
- Provide protection from malicious code at appropriate locations
- Monitor information security alerts and advisories

To read these government contracting regulations in their entirety visit: DFARS 252.204 and NIST SP 800-171

For more information on government contracting visit: Department of Defense Office of

Small Business

To determine whether your business has met the requirements for government contracting visit: Cybersecurity Evaluation Tool and NIST Self-Assessment Handbook

To receive help with government contracting visit: Procurement Technical Assistance Center or Find Your Local SBDC

More on Cybersecurity for Small Businesses

To continue learning about Cybersecurity for Small Businesses, view our next section: General Cybersecurity Resources & Contacts

Additional Small Business Resources

Already in business or thinking about starting your own small business? Check out our various Small Business Snapshots, Market Research Links and our Sample Business Plans collection. Remember, you can also receive free professional business advice and free or low-cost business training from your local Small Business Development Center!

Sharing is caring!

- Share
- Tweet
- LinkedIn