Department of Defense Cybersecurity Requirements:

What Businesses Need to Know?

Why is Cybersecurity important to the Department of Defense?

Today, more than ever, the Department of Defense (DoD) relies upon external contractors and suppliers to carry out a wide range of missions. Sensitive data is shared with these companies and must be protected. Inadequate safeguards of this sensitive data may threaten America's national security and put service members lives at risk.

What has DoD done to address this issue?

DoD has implemented a basic set of cybersecurity controls through DoD policies and the Defense Federal Acquisition Regulation Supplement (DFARS). The DFARS rules and clauses apply to the safeguarding of contractor/supplier information systems that process, store or transmit Controlled Unclassified Information (CUI). https://www.archives.gov/cui/registry These security controls must be implemented at both the contractor and subcontractor levels based on information security guidance developed by the National Institute of Standards and Technology (NIST) Special Publication 800-171 "Protecting Controlled Unclassified Information in Non-federal Information Systems and Organizations."

How does this affect small businesses?

DoD contractors and suppliers (including small businesses) must adhere to two basic cybersecurity requirements:

> (1) They must 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) They must rapidly report cyber incidents and cooperate with DoD to respond to these security incidents, including access to affected media and submitting malicious software.

What is *adequate security*?

The set of minimum cybersecurity standards are described in NIST Special Publication 800-171 and broken down into fourteen areas:

Access Control Media

Awareness & Training

Audit & Accountability

Configuration Management

Identification & Authentication

Incident Response

Maintenance

Media Protection

Personnel Security

Physical Protection

Risk Assessment

Security Assessment

System & Communications Protection

System & Information Integrity

In each of these areas, there are specific security requirements that DoD contractors/suppliers must implement.

What is the deadline?

Full compliance was initially required no later than **December 31, 2017**. The contractor/supplier were to notify the DoD CIO within 30 days of contract award, of any security requirements not implemented at the time of contract award. They can propose alternate, equally effective, measures to DoD's CIO through their contracting officer

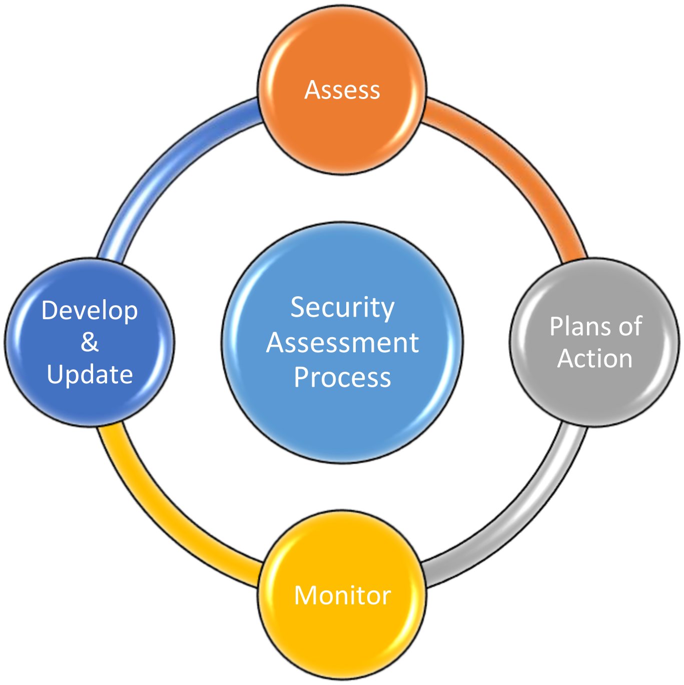
If DoD determines that other measures are required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability, contractors may also be required to implement additional security precautions.

How do small businesses attain these standards?

NIST SP 800-171 can be found at:

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

SP 800-171 references another document (NIST Special Publication 800-53) which goes into more detail about the security controls. In addition, NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems", Sections 3.3 to 3.6 may provide small business a systematic step-by-step approach to implementing, assessing and monitoring the controls.



How do I meet the SP 800-171 Requirements?

Meeting the SP 800-171 is not a one-time fix, rather it is a continuous assessment, monitoring and improvement process. Periodically assess the security controls in your company's systems to determine if the controls are effective in their application. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in systems. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

Although these requirements may initially seem overwhelming, small businesses can use this framework to divide the project into small, manageable chunks and work toward attaining compliance. Incurred costs may also be recoverable under a cost reimbursement contract pursuant to FAR 31.201-2.

May small businesses outsource these requirements?

Small businesses may use subcontractors and/or outsource information technology requirements, but they are responsible for ensuring that these entities they use meet the cybersecurity standards. If they anticipate using cloud computing, they should ensure the cloud service meets FedRAMP “moderate” security requirements and complies with incident reporting, media, and malware submission requirements.

What if there is a potential breach?

Don’t panic. Cybersecurity occurs in a dynamic environment. Hackers are constantly coming up with new ways to attack information systems and DoD is constantly responding to these threats. So, even if you do everything right and institute the strongest checks and controls, it is possible that someone will come up with a new way to penetrate these measures. DoD does not penalize small businesses acting in good faith. The key is to work in partnership with DoD so that new strategies can be developed to stay one step ahead of the hackers.

Contact DoD immediately . Bad news does not get any better with time. These attacks threaten America’s national security and put service members lives at risk. DoD should respond quickly to change operational plans and to implement measures to respond to new threats and vulnerabilities So, small businesses should report any potential breaches to DoD within **seventy-two (72) hours** of discovery of any incident. Report these incidents directly on-line: **https://dibnet.dod.mil/** Interpret potential breaches broadly to include all actions taken using computer networks that result in actual or potentially adverse effects on information systems and/or the information residing therein. These include “possible ex-filtration, manipulation, or other loss or compromise of controlled technical information from an unclassified information system” and “any unauthorized access to an unclassified information system on which such controlled technical information is resident or transiting.”

Be helpful and transparent. Businesses must also cooperate with DoD to respond to these security incidents. They should immediately preserve and protect all evidence and capture as much information about the incident as possible. They should review their networks to identify compromised computers, services, data, and user accounts and identify specific covered defense information that may have been lost or compromised.

What is a System Security Plan?

A document that describes how a small manufacturer meets the security requirements for a system or how a small manufacturer plans to meet the requirements. The system security plan describes the system boundary; the environment in which the system operates; how the security requirements are implemented; and the relationships with or connections to other systems

What are Plans of Action?

A small manufacturer should develop Plans of Action that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented. Companies can document the system security plan and plan of action as separate or combined documents and in any chosen format.

When requested, the System Security plan and any associated Plans of Action for any planned implementations or mitigations should be submitted to the responsible federal agency/contracting officer. The Plans of Action help to demonstrate implementation or planned implementation of the security requirements. Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system.

Where can businesses get additional help?

Cyber Management Systems can provide additional guidance on meeting the NIST SP 800-171 requirements. Please contact us for a free assessment.

Cyber Management Systems

1-866-CYBERMS (866-292-3767)

https://cybermanagementsystems.com