

DEFENSE CYBERSECURITY REQUIREMENTS: WHAT SMALL BUSINESSES NEED TO KNOW



Office of Small Business Programs, U.S. Department of Defense
3600 Defense Pentagon, Room 3E185, Washington, DC 20301-3600

Why is cybersecurity important?

Today, more than ever, the Department of Defense (DoD) relies upon external contractors to carry out a wide range of missions and shares sensitive data with these entities. Inadequate safeguards threaten America's national security and put servicemembers lives at risk.

What has DoD done to address this issue?

In April 2009, the DoD and DNI CIOs launched the Joint Task Force Transformation Initiative to develop a comprehensive set of cybersecurity standards and align the publications produced by different federal agencies. Over the years, Congress added more requirements in the National Defense Authorization Act (NDAA), the National Institute of Standards and Technology (NIST) produced several iterations of cybersecurity standards, and DoD implemented these measures through changes to DoD policies and the Defense Federal Acquisition Regulation Supplement (DFARS).

How does this affect small businesses?

Under the interim rule issued in December 2015 (DFARS § 252.204-7012), DoD contractors (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 break down into fourteen areas:

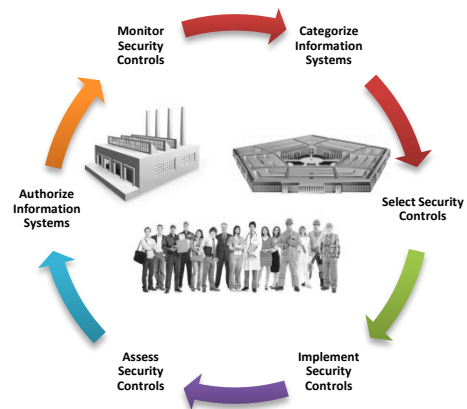
Access Control	Media Protection
Awareness & Training	Personnel Security
Audit & Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification & Authentication	Security Assessment
Incident Response	System & Com Protection
Maintenance	System & Info Integrity

In each of these areas, there are specific security requirements that DoD contractors must implement. Full compliance is required not later than December 31, 2017. The contractor must 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?

The standards reference another document (NIST Special Publication 800-53) which goes into more detail about the 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 businesses a systematic step-by-step approach to implementing, assessing and monitoring the controls :



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 contractors outsource these requirements?

Contractors 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?

- (1) 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 a contractor does everything right and institutes 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 contractors 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.
- (2) Contact DoD immediately. Bad news does not get any better with time. These attacks threaten America's national security and put servicemembers lives at risk. DoD has to respond quickly to change operational plans and to implement measures to respond to new threats and vulnerabilities. So, contractors should report any potential breaches to DoD within seventy-two hours of discovery of any incident. Report these incidents directly online:

<http://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 exfiltration, 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. Contractors must also cooperate with DoD to respond to these security incidents. Contractors 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.

Where can small businesses get additional help?

DoD's OSBP has put together a comprehensive list of cybersecurity resources for small businesses on its website:

<http://business.defense.gov/Resources.aspx>

Each individual service component and defense agency also has an office dedicated to assisting small businesses:

U.S. Army:	(703) 695-3220
Pamela Monroe	<pamela.l.monroe8.civ@mail.mil>
U.S. Navy:	(202) 685-6485
Brad Taylor	<brad.taylor@navy.mil>
U.S. Air Force:	(571) 256-7756
David Sikora	<david.l.sikora.civ@mail.mil>
DCMA:	(214) 573-2168
Shelly Thomas	<shelly.thomas@dla.mil>
DHA:	(703) 681-7046
Dan Duckwitz	<daniel.m.duckwitz.civ@mail.mil>
DIA:	(202) 231-2166
Maria Kersey	<maria.kersey@dodis.mil>
DLA:	(703) 767-1657
Trish Culbreth	<patricia.culbreth@dla.mil>
MDA:	(256) 450-5281
Ruth Dailey	<ruth.dailey@mda.mil>
NGA:	(571) 557-7223
Diana Hughes	<diana.m.hughes@nga.mil>
NSA:	(443) 479-2467
Jim Higgins	<jehiggi@nsa.gov>

I hope this information has been helpful. If you have any questions or concerns, please feel free to reach out to my office at (571) 372-6191.



Kenyata L. Wesley

Acting Director, Office of Small Business Programs
U.S. Department of Defense