Cybersecurity and Compliance when working with Government Agencies

What Small Businesses Need to Know – Source https://business.defense.gov/Small-Business/Cybersecurity/

The threats facing DoD's unclassified information have dramatically increased as we provide more services online, digitally store data and rely on contractors for a variety of information technology services. Recent high-profile incidents involving government information demand that information system security requirements are clearly, effectively and consistently communicated to both government and industry.

There are two types of information systems that process or store DoD's unclassified information:

1. Contractor's Internal Information System: An information system that is owned, or operated by or for, a contractor.

2. DoD Information System, to include:

DoD-owned and/or operated Information System: An information system owned or operated by the DoD or by another government organization on behalf of the DoD.

Contractor System operated on behalf of DoD: The term "on behalf of" as used here means when a contractor builds an information system for the DoD or operates an information system for the DoD, e.g., an email provider or payroll system, or provides processing services for DoD. e.g., cloud-service providers.

The protections required to protect government information are dependent on the information we are protecting and the kind of system on which the information is processed or stored.

What is DoD doing to protect DoD information processed, stored or transiting a contractor's internal Information System?

Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, was published as a final rule Oct. 21, 2016.

How does this affect small businesses?

DFARS Clause 252.204-7012 requires DoD contractors, including small businesses, to:

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.

2. Rapidly report cyber incidents to DoD at https://dibnet.dod.mil.

3. When contractors or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer.

4. Preserve and protect images of all known affected information systems identified and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

What is adequate security?

Minimum cybersecurity standards are described in NIST Special Publication 800-171 and break down into the following 14 areas:

Access Control

Awareness & Training

Audit & Accountability

Configuration Management

Identification & Authentication

Incident Response

Maintenance

Media Protection

Maintenance

Personnel Security

Physical Protection

Risk Assessment

System & Communication Protection

System & Info Integrity

In each of these areas, there are specific security requirements that DoD contractors must implement. Full compliance is required no later than December 31, 2017. Contractors must notify the DoD CIO within 30 days of contract award of any security requirements not implemented at the time of contract award. Contractors 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 provides 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.

Will the DoD certify that a contractor is 100 percent compliant with NIST SP 800-171?

The rule does not require "certification" of any kind, either by DoD or any other firm professing to provide compliance, assessment or certification services for DoD or contractors. Nor will DoD recognize third-party assessments or certifications. By signing the contract, the contractor agrees to comply with the terms of the contract.

Is a third-party assessment of compliance required?

Some companies with limited cybersecurity expertise may choose to seek outside assistance in determining how best to meet and implement the NIST SP 800-171 requirements in their company. But once the company has implemented the requirements, there is no need to have a separate entity assess or certify that the company is compliant with NIST SP 800-171.

May contractors outsource these requirements?

Contractors may use subcontractors and/or outsource information technology requirements, but they are responsible for ensuring that the 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. 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.

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. Contractors should report any potential breaches to DoD within 72 hours of discovery of any incident.

Report incidents directly online at 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 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.

Feel overwhelmed or need help implementing a security program?

AMS Technology can help. With over 30 years of experience and the tools and services to help you become compliant, we can get you to compliance quickly and without breaking the bank. Our EDRProtect program along with the Enterprise Managed Service program, we can make your network **Safe, Reliable, and Compliant.**