VIP Presents

Roadmap to DFARS Compliance
Will your business be ready for the 12/31/17 Deadline?
The VIP Program

• Accelerating the Growth of Veteran Owned Small Businesses in the Federal Marketplace

Powered By

SBA
U.S. Small Business Administration
Office of Veterans Business Development
"Only five years after graduating, SAMS debuted at #761 on the Inc. 5000 Fastest Growing Companies. VIP was instrumental to our success."

Staci Redmon, President/CEO
Strategy and Management Services, Inc., SDVOSB
Winner, SBA’s “Small Business Person of the Year,” 2016
The VIP Program

• **Accelerate Success in the Federal Space**
  – 3-day, 27-hour comprehensive certification program
  – Bolger Center, 11 miles from the White House
  – No cost for training, hotel, meals (travel not included)
DFARS Compliance Overview
Technology Risk Services
### Background

The federal information supply chain includes federal and non-federal information systems operated by its contractors entrusted with federal information.

### Spending

In FY 2016 the federal government spent $92B on Information Technology (IT) systems and applications.

### Information Technology

The government conducts a lot of its business using these IT systems which includes working with sensitive classified and unclassified information.

### Supply Chain

The federal information supply chain includes federal and non-federal information systems operated by its contractors entrusted with federal information.

### Threat Vectors

Federal IT systems and data are constantly targeted by domestic and foreign threat actors.

### FUN FACTS

- The government conducts a lot of its business using these IT systems which includes working with sensitive classified and unclassified information.
- Federal IT systems and data are constantly targeted by domestic and foreign threat actors.
Background

- Department of Defense (DoD) information is especially sensitive and DoD is committed to protecting information within its own systems and its information supply chain which is mostly maintained by contractors.

- DoD has increasingly used its authority over acquisition methods and contract requirements to improve cybersecurity and information assurance of nonfederal information systems.

- The Defense Federal Acquisition Regulation Supplement (DFARS) provisions & clauses demonstrate how “acquisition planning and contract administration” are used to:
  1) require National Institute of Standards & Technology (NIST) Special Publication 800-171 security controls &
  2) establish cyber incident reporting procedures to secure the DoD information supply chain.
What are the Clauses and Provisions?

252.204-7008 – “Compliance with Safeguarding Covered Defense Information Controls”
- This is a provision, which is a written term or condition used only in solicitations and applies only before contract award.

252.204-7012 – “Safeguarding Covered Defense Information and Cyber Incident Reporting”
- This is a clause which is a term or condition used in contracts and solicitations. It applies after contract award, or both before and after award.
- If the 252.204-7008 provision is in the solicitation language then the clause 252.204-7012 will be included in the contract language.
What is Covered Defense Information (CDI)?

**What is CDI?**
CDI is any unclassified information that is provided to the contractor by or on behalf of DoD in connection with the performance of the contract or collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

CDI has a broad definition and can be technical, administrative, or operational in nature.

CDI can fall in any of the following categories:
- Unclassified Controlled Technical Information
- Critical information
- Export control
- Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies (e.g., privacy, proprietary business information).
Does DFARS apply to my organization?

If you answer “yes” to any of these questions then DFARS requirements apply to your organization.

☑ Is your organization a DoD Contractor? (very likely)

☑ Does your company work with CDI/Unclassified Controlled Technical Information (UCTI)? (absolutely)

☑ Is DFARS provision 252.204-7008 in the language of a solicitation your are bidding on? (absolutely)

☑ Is DFARS clause 252.204-7012 used in your existing contract requirements? (absolutely)
Does the regulation flow down to subcontractors?

- All companies in the federal information supply chain that may have access to CDI are covered under the DFARS 252.204-7012 compliance requirements, it therefore applies to all subcontractors.

- Smaller subcontractors could possibly present additional risk as they may not have a robust information security program and hence may not have adequate security controls.
Does it apply to Cloud Service Providers (CSP)?

- If a contractor uses a CSP to meet a DoD contract requirement, the CSP should meet security requirements equivalent to those established by the government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline.

- The CSP as a subcontractor will need to meet with requirements of the DFARS 252.204-7012 for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.
What Control Framework Should We Use?

- NIST SP 800-171: *Protecting Controlled Unclassified Information in Nonfederal Information Systems & Organizations* is the required control framework.

- NIST SP 800-171 is a subset of NIST SP 800-53 control framework.
  - 110 controls derived from NIST SP 800-53 provide specific requirements for access control, awareness and training, auditing, configuration management, communications protection and more.

- Some controls may be met through process or policy; some may require a technology solution.
## What are the NIST SP 800-171 Control Families?

<table>
<thead>
<tr>
<th>NIST 800-171 Control Families</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Control</strong> (22)</td>
</tr>
<tr>
<td><strong>Awareness and Training</strong> (3)</td>
</tr>
<tr>
<td><strong>Audit and Accountability</strong> (9)</td>
</tr>
<tr>
<td><strong>Configuration Management</strong> (9)</td>
</tr>
<tr>
<td><strong>Identification and Authentication</strong> (11)</td>
</tr>
<tr>
<td><strong>Incident Response</strong> (3)</td>
</tr>
<tr>
<td><strong>Maintenance</strong> (6)</td>
</tr>
</tbody>
</table>
What are the Consequences for Non-Compliance?

- Per DFARS 252.204-7012, (b) (ii) (A) “The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017.”
- Non-compliant contractors may be debarred or disqualified from any new DoD contracts.
- DoD contractors will therefore select their subcontractors and teaming partners with great care to avoid being considered non-compliant.
- Contractors that do comply will have a competitive edge over their non-compliant competitors.
What is the Cost of Compliance for My Organization?

- The cost of DFARS 252.204-7012 compliance is considered an allowable cost under Federal Acquisition Regulation (FAR)/Cost Accounting Standards (CAS)
- Aronson can provide guidance on whether you are eligible to recover these costs
Are There Any Allowable Exemptions?

DFARS 252.204-7012 allows for the contractor to identify situations in which a required control might not be necessary or for an alternative to a required control.

The contractor should provide a written explanation describing the reasons why a control is not required or adequate security is provided by an alternative control and protective measure.

Subcontractors must notify the Primary Contractor (or next higher-tier subcontractor) when submitting a request to the Contracting Officer of a variance from a NIST SP 800-171 security requirement.

The DoD Chief Information Officer (CIO) will decide on the exemption request, which is submitted initially to the Contracting Officer.
What are the Cyber Incident Reporting Requirements?

DFARS 252.204-7012 requires a contractor to report a cyber incident to DoD within 72 hours of discovering such an incident using the DIBNet portal.

Contractors and subcontractors will need to obtain a DoD-approved medium assurance certificate to report cyber incidents.

Aronson can assist with crafting a comprehensive & compliant Cyber Incident Response Plan along with documented Incident Response procedures.
Roadmap to Compliance

Assessment & Status Report

- CDI must be identified & marked appropriately throughout the data management life cycle whether in agency or contractor custody.
  - NIST 800-171 compliance due by 12/31/17 & “adequate security” required immediately.
  - Contractors must notify the DoD CIO of any 800-171 controls not implemented within 30 days from the award date.

Remediate

- Complete remediation of any gaps identified during the assessment (includes subcontractors) to meet the 12/31/17 compliance due date.
- Implement controls to meet cyber incident reporting requirements.
  - Acquire DoD-approved medium access for reporting & communicating about cyber incidents.
  - Notify designated personnel within 72 hours of incident discovery.

Continuous Monitoring

- On a periodic basis monitor the design and operating effectiveness of controls to ensure that they are functioning as intended.
THANKS!

Any Questions?
The VIP Program

Thank you for attending the VIP Webinar

• There will be a short survey at the conclusion of the webinar. Your opinion and feedback are very important in continuing the webinar series. Please take moment and complete the 5 question survey