As the Department of Defense implements new policies and regulations governing industry’s cyber practices in an effort to fortify its cyber vulnerabilities, it is vital to collect and consider the views of the defense industrial base. As the voice of the defense industry, NDIA is uniquely situated to tap into the breadth of our membership for its perspective on the current cybersecurity landscape. The following presentation is the result of a cyber survey conducted in conjunction with NDIA’s San Diego Chapter from April – June 2019. This survey sought to gauge industry’s perspective on recent Defense Federal Acquisition Regulation Supplement (DFARS) changes, its view on the cost of cyber compliance, and the current methods of cyber protection being used by industry.

**KEY TAKEAWAYS**

- 26 percent of participants have been a victim of a successful cyber attack
- 75 percent of Prime contractors believe their subcontractors are not in compliance with DFARS 7012
- 21 percent of participants feel that implementing DFARS 7012 will result in no improvement to their overall security

**TOP THREE BIGGEST CYBER THREATS FACING INDUSTRY:**

1. Cyberattack by an outside actor
2. Disgruntled or former employee wrecking internal systems
3. Major security breach that impacts company personnel

**What security measures does your company use?**

- We use a firewall
- We use two-factor or multi-factor authentication for log-ons
- We require VPN usage for remote work
- We use access security at the workspace in addition to door locks
- We have a dedicated in house IT person or department
- We have a dedicated email server
- We rely on anti-virus software that came installed on our equipment
- We outsource most of our IT support to an external provider
- We self-service but do not have staff dedicated
- We host our own website

**“We view security costs as part of our corporate overhead that we factor into our DoD pricing.”**

Survey participants were asked to rate their agreement with the statements above on a scale of 0-100.

**“We view DFARS 7012 costs as part of our corporate overhead that we factor into our DoD pricing.”**
Has your company ever been the victim of a successful cyber attack?

If you are a prime contractor, is (are) your subcontractor(s) in compliance with DFARS 7012 regulations?

If you are a subcontractor, has (have) your prime contractor(s) provided you with information about how to comply with the DFARS 7012 regulations?

How prepared, do you believe, is your company to comply with the DFARS 7012 requirements?

How confident are you in your ability to recover from a cyber incident in 24 hours?

Survey participants were asked to rate their agreement with the statements above on a scale of 0-100.
How adequate do you think the DFARS 7012 and NIST SP 800-171 guidance is to achieve a comprehensive level of security?

Other Than Small Business

Small Business

Survey participants were asked to rate their agreement with the statements above on a scale of 0-100.

Rate your level of preparedness for a Defense Contract Management Agency (DCMA) cybersecurity audit.

Other Than Small Business

Small Business

Survey participants were asked to rate their level of preparedness on a scale of 0-100.

How much do you agree with this statement? “Our employees are well prepared to understand and respond to cybersecurity threats.”

Other Than Small Business

Small Business

Survey participants were asked to rate their level of preparedness on a scale of 0-100.

How much do you agree with this statement? “Our senior management has communicated that 7012 compliance is a priority.”

Other Than Small Business

Small Business

Survey participants were asked to rate their agreement with the statement above on a scale of 0-100.
47% have not attended any outside education or training for DFARS 7012 requirements.

29% have attended DFARS 7012 requirements education or training at an industry conference.

18% have attended DFARS 7012 requirements education or training from a commercial security training provider.

17% have attended DFARS 7012 requirements education or training from an external consultant SME.

14% have attended DFARS 7012 requirements education or training from an internal SME.

14% have attended DFARS 7012 requirements education or training at their local NDIA chapter.

12% have attended DFARS 7012 requirements education or training at their local PTAC and/or NIST MEP Center.

8% have attended DFARS 7012 requirements education or training at Defense Acquisition University.

7% have attended DFARS 7012 requirements education or training from their prime contractor.

How much, do you believe, will the DFARS 7012 requirements help DoD’s operational security?

- No improvement – my company’s security is better than our customers’ security
- No improvement – it doesn’t matter what vendors do. A determined adversary is going to achieve their goals against DoD
- Big improvement – these regulations really improve the overall security landscape for DoD

PARTICIPANT PROFILE
This survey was distributed through email, social media, and posted on the NDIA website. NDIA’s survey attracted a wide array of respondents employed in the defense industrial base and defense acquisitions. Respondents included employees of both subcontractors and prime contractors, academia, and those involved in other areas of the defense acquisition process. In total, the survey collected 285 responses.

COMPANY SIZE PROFILE

<table>
<thead>
<tr>
<th>Number of Employees</th>
<th>Percentage of Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 to 50</td>
<td>34%</td>
</tr>
<tr>
<td>51 to 250</td>
<td>19.5%</td>
</tr>
<tr>
<td>251 to 500</td>
<td>5%</td>
</tr>
<tr>
<td>501 to 1000</td>
<td>6%</td>
</tr>
<tr>
<td>1001 to 2000</td>
<td>5%</td>
</tr>
<tr>
<td>2001 +</td>
<td>30%</td>
</tr>
</tbody>
</table>

FOR MORE INFORMATION, CONTACT
Regulatory@NDIA.org or visit NDIA.org/Divisions/Cybersecurity