2019 Cybersecurity Report

Beyond Obfuscation: The Defense Industry’s Position within Federal Cybersecurity Policy
About the Report

• Section I: Illustrations of Cyber Threats and Vulnerabilities
• Section II: Policy Response to Cyber Risk
• Section III: Industry’s Perspective (Survey Analysis)
• Section IV: Conclusions and Recommendations

• Released: August 2019

• Available online at: NDIA.org/CyberStudy2019
SECTION III: INDUSTRY’S PERSPECTIVE
(SURVEY ANALYSIS)
Methodology

- Online Survey Developed with NDIA San Diego Chapter
- Distributed via Email & NDIA Website
- Responses Collected for 60 Days
- Approximately 300 Responses Collected
  - Participation was not limited to NDIA members
Demographics

Location Distribution

PRIMARY INDUSTRY

- Technology
- Services
- Manufacturing
- Other
Company Financials

• **Key Takeaways**
  
  – Subcontractors are less dependent upon revenue from the Department of Defense than prime contractors
  
  – Small businesses have less diversified revenue streams than larger businesses

<table>
<thead>
<tr>
<th>Percent of Business Revenue derived from DoD</th>
<th>0-20 percent</th>
<th>21-40 percent</th>
<th>41-60 percent</th>
<th>61-80 percent</th>
<th>81-100 percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prime Contractors</td>
<td>5 percent</td>
<td>11 percent</td>
<td>12 percent</td>
<td>20 percent</td>
<td>52 percent</td>
</tr>
<tr>
<td>1st Tier Subcontractors</td>
<td>19 percent</td>
<td>11 percent</td>
<td>11 percent</td>
<td>17 percent</td>
<td>43 percent</td>
</tr>
<tr>
<td>2nd Tier Subcontractors</td>
<td>46 percent</td>
<td>31 percent</td>
<td>0 percent</td>
<td>0 percent</td>
<td>23 percent</td>
</tr>
<tr>
<td>3rd Tier Subcontractors</td>
<td>60 percent</td>
<td>20 percent</td>
<td>0 percent</td>
<td>0 percent</td>
<td>20 percent</td>
</tr>
<tr>
<td>Processor</td>
<td>0 percent</td>
<td>50 percent</td>
<td>25 percent</td>
<td>0 percent</td>
<td>25 percent</td>
</tr>
<tr>
<td>Other-than-small</td>
<td>14 percent</td>
<td>12 percent</td>
<td>14 percent</td>
<td>23 percent</td>
<td>38 percent</td>
</tr>
<tr>
<td>Small</td>
<td>13 percent</td>
<td>15 percent</td>
<td>9 percent</td>
<td>12 percent</td>
<td>52 percent</td>
</tr>
</tbody>
</table>
Information Technology

- **Key Takeaways**
  - Large businesses employ more security measures than small businesses
  - Small businesses are more reliant on external information security solutions
  - Use of personal devices is much more prevalent among small business employees

What Security Measures Does Your Company Use?

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

#### Data Storage Methods

- **Commercial cloud service**
- **Internally-owned cloud server**
- **Offsite**
- **Onsite**
- **Server provided by managed-services company**
- **Internally-owned network storage**
- **An external drive**
- **Personal-use desktop or laptop only**

#### Device Use Policy

- **Use Government-issued devices**
- **Let employees use their own mobile phones, laptops or tablets for corporate purposes**
- **Issue corporate mobile phones, laptops or tablets for mobile use**
COST ESTIMATING AND ACCOUNTING

• Key Takeaways
  – The majority of respondents view security-related costs as a cost-driver when pricing contract bids
  – Industry supports treating costs associated with carrying out DFARS 7012 requirements as direct costs
  – Nearly half of respondents have not estimated the cost of DFARS 7012 compliance
“We view security costs as part of our corporate overhead that we factor into our DoD pricing.”

“We view DFARS 7012 costs as part of our corporate overhead that we factor into our DoD pricing.”
Corporate Opinions

• Key Takeaways
  – 44 percent of companies with greater than 500 employees have been the victim of a cyber attack
  – Of a list of potential cyber-related threats, respondents are least concerned about having a contract rescinded by a prime contractor or contracting officer as a result of a cyber incident
  – Small business does not have an adequate sense of the cost of responding to or recovering from a cyber incident
  – 44 percent of prime contractors do not have documentation of a system security plan (SSP) from their subcontractor(s)
Corporate Opinions

Has your company ever been the victim of a successful cyber attack?

Other Than Small Business:
- Yes: 44%
- Unsure: 28%
- No: 28%

Small Business:
- Yes: 18%
- Unsure: 8%
- No: 74%
Corporate Opinions

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

Other Than Small Business

Small Business
Corporate Opinions

COMPLIANCE WITH DFARS 7012

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

- 26% Yes, we have a documented SSP from the subcontractor
- 25% We have requested an SSP from the subcontractor
- 11% Definitely – our prime(s) has (have) provided information on how to comply and has (have) accessible for questions and discussion
- 44% No, we do not currently have a documented System Security Plan (SSP) from the subcontractor
- 6% Not at all – we do not handle controlled unclassified information (CUI)
- 5% No, and we have taken corrective action against the subcontractor

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

- 6% No – we saw it as a flow-down in our subcontract
- 40% Yes – our prime(s) made us aware of the requirement
- 43% Not at all – we do not have access to the information
- 11% Definitely – our prime(s) has (have) provided information on how to comply and has (have) accessible for questions and discussion
## USE OF CYBERSECURITY EDUCATIONAL RESOURCES

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>47%</td>
<td>have not attended any outside education or training for DFARS 7012 requirements.</td>
</tr>
<tr>
<td>29%</td>
<td>have attended DFARS 7012 requirements education or training at an industry conference.</td>
</tr>
<tr>
<td>18%</td>
<td>have attended DFARS 7012 requirements education or training from a commercial security training provider.</td>
</tr>
<tr>
<td>17%</td>
<td>have attended DFARS 7012 requirements education or training from an external consultant SME.</td>
</tr>
<tr>
<td>14%</td>
<td>have attended DFARS 7012 requirements education or training from an internal SME.</td>
</tr>
<tr>
<td>14%</td>
<td>have attended DFARS 7012 requirements education or training at their local NDIA chapter.</td>
</tr>
<tr>
<td>12%</td>
<td>have attended DFARS 7012 requirements education or training at their local PTAC and/or NIST MEP Center.</td>
</tr>
<tr>
<td>8%</td>
<td>have attended DFARS 7012 requirements education or training at Defense Acquisition University.</td>
</tr>
<tr>
<td>7%</td>
<td>have attended DFARS 7012 requirements education or training from their prime contractor.</td>
</tr>
</tbody>
</table>
REPORT RECOMMENDATIONS
Recommendations for Government

• Increased communication between industry partners with a focus on small business
• Right-size the flow of information to industry
• Simplifying the current cyber regulatory regime
Recommendations for Industry

• Prime contractors must share best practices and experiences with lower-tier companies while working with government to manage the flow of sensitive information within the supply chain

• Smaller businesses need to make a more intentional effort to adopt cyber fortifications and ensure compliance with current cyber regulations

• All of industry must commit to working with government as the new CMMC program is developed to ensure that the new set of regulations is as effective as possible without an unduly burden on industry
QUESTIONS?

Corbin Evans, Director of Regulatory Policy
CEVANS@NDIA.ORG
(703) 247 – 2598