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

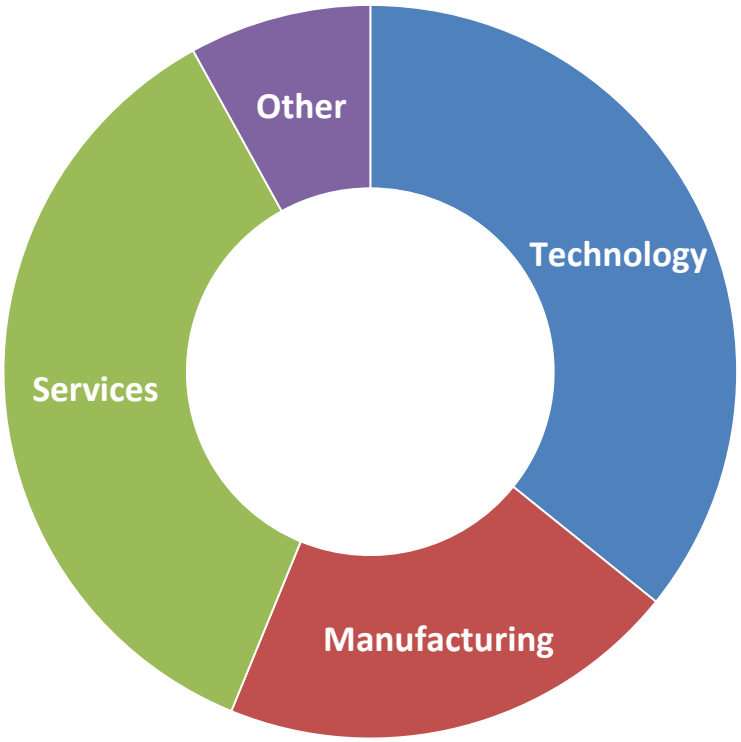
SECTION III: INDUSTRY'S PERSPECTIVE
(SURVEY ANALYSIS)

Methodology

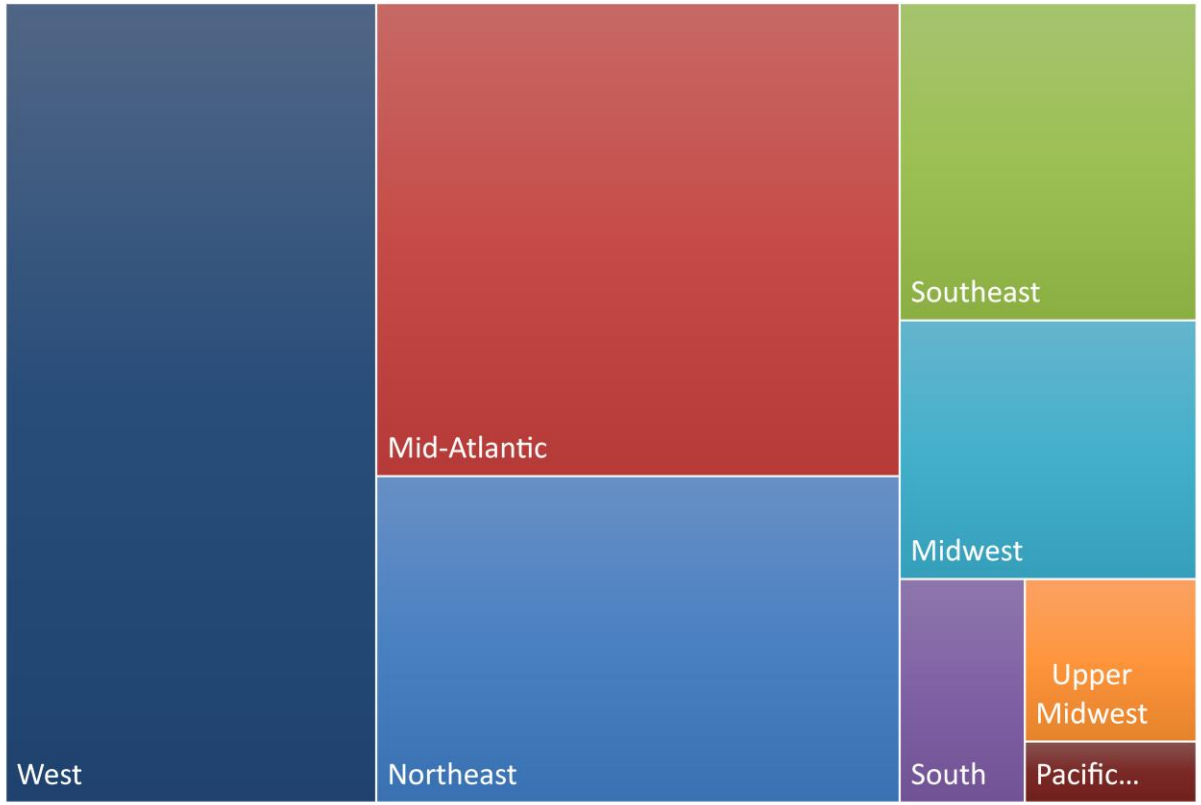
- **Online Survey Developed with NDIA San Diego Chapter**
- **Distributed via Email & NDIA Website**
- **Responses Collected for 60 Days**
- **Approximately 300 Responses Collected**
  - Participation was not limited to NDIA members

Demographics

PRIMARY INDUSTRY

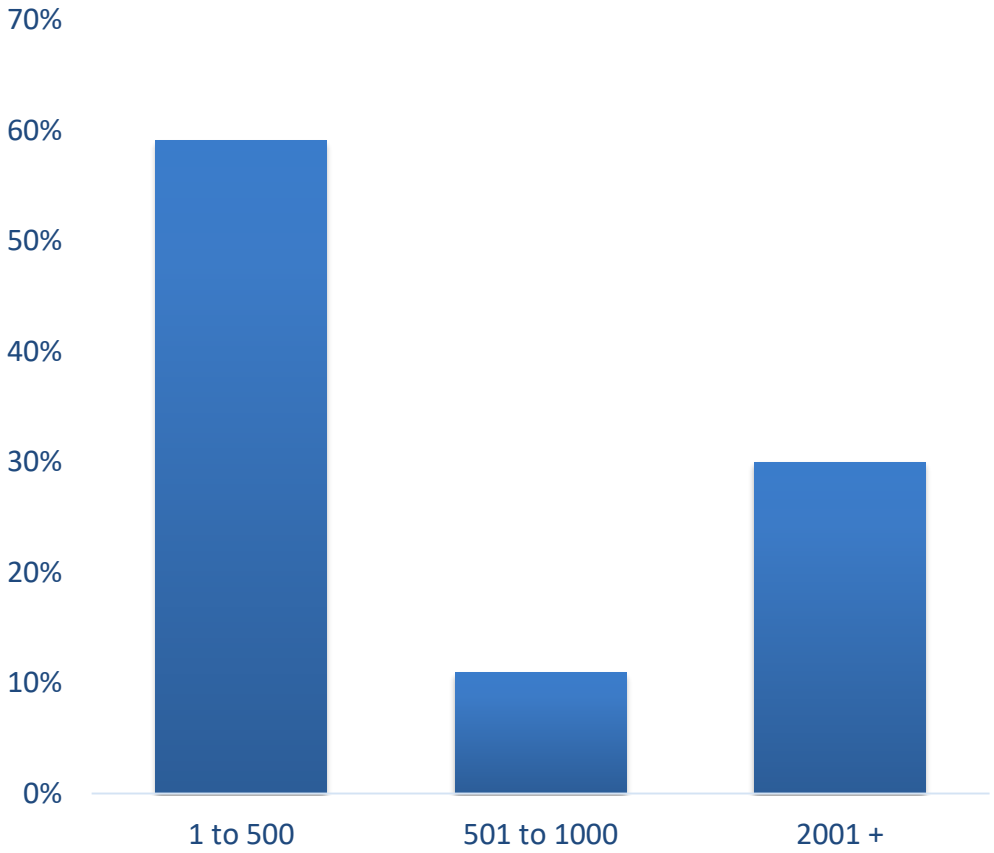


Location Distribution

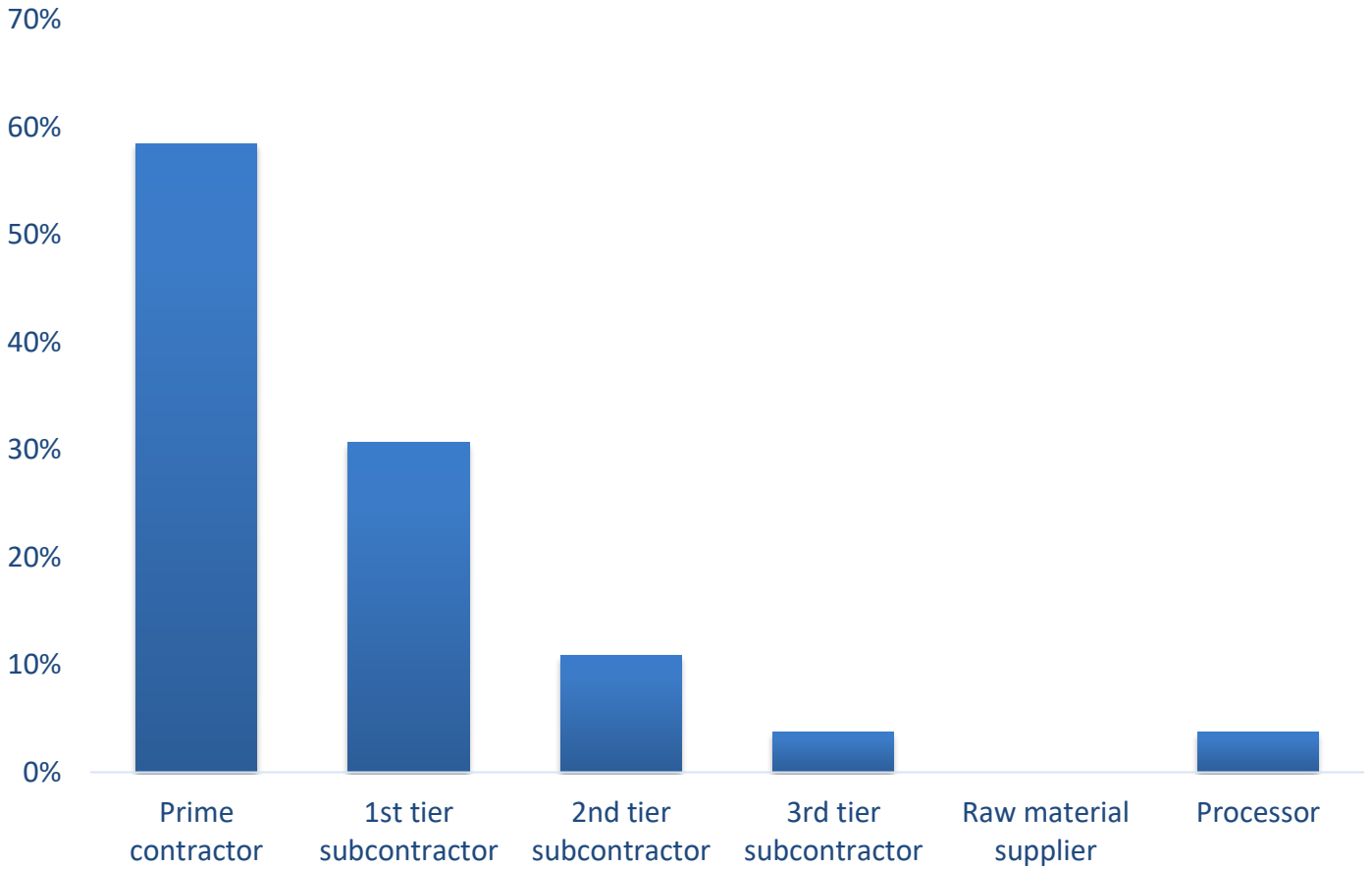


Demographics

Number of Employees



Primary Position in the Supply Chain



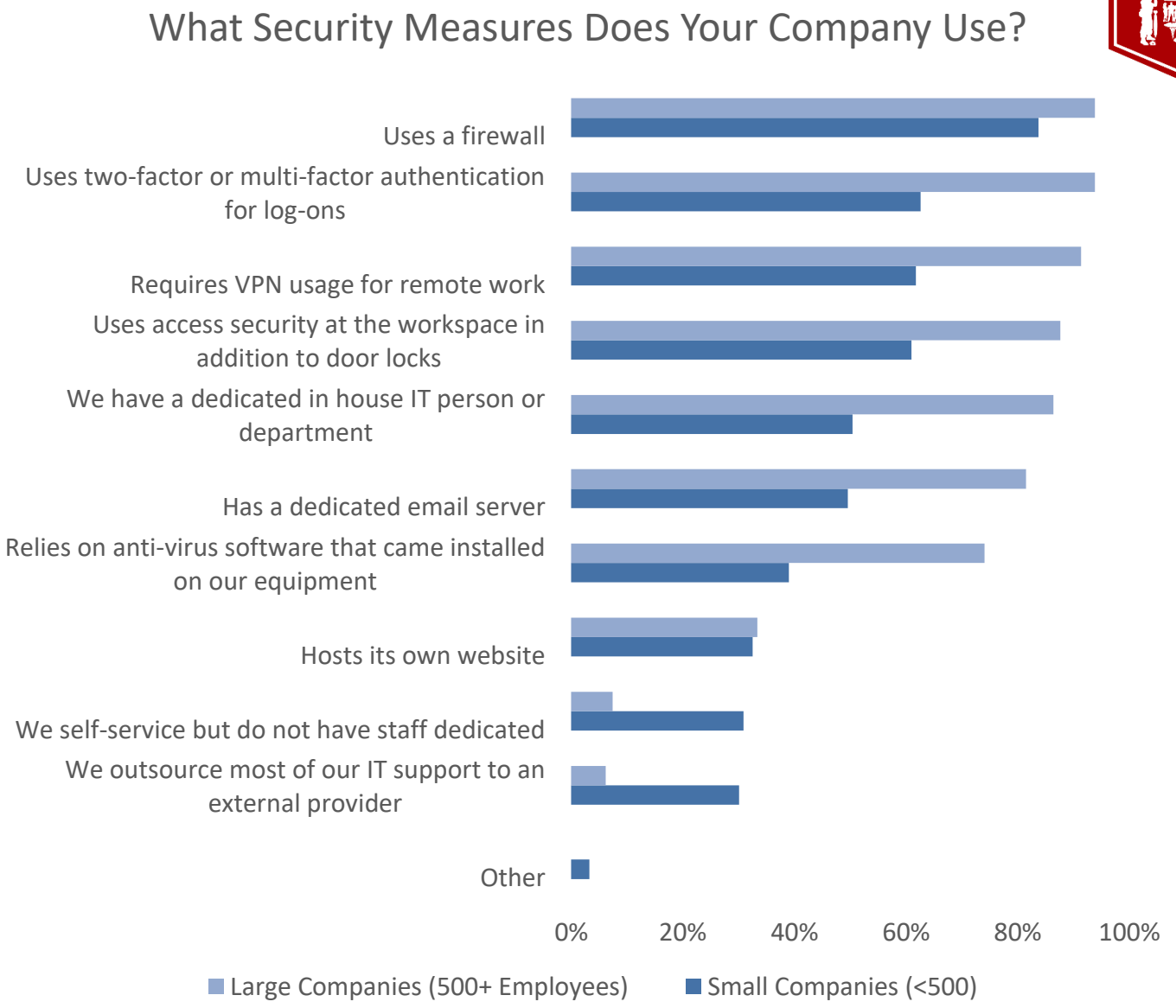
Company Financials

- **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

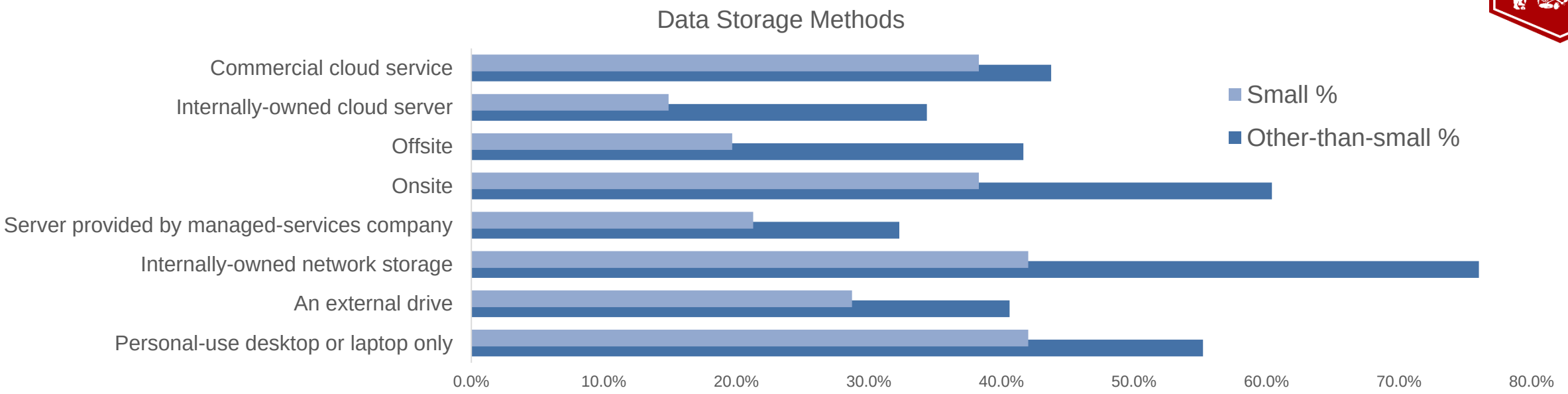
Percent of Business Revenue derived from DoD					
	0-20 percent	21-40 percent	41-60 percent	61-80 percent	81-100 percent
Prime Contractors	5 percent	11 percent	12 percent	20 percent	52 percent
1st Tier Subcontractors	19 percent	11 percent	11 percent	17 percent	43 percent
2nd Tier Subcontractors	46 percent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

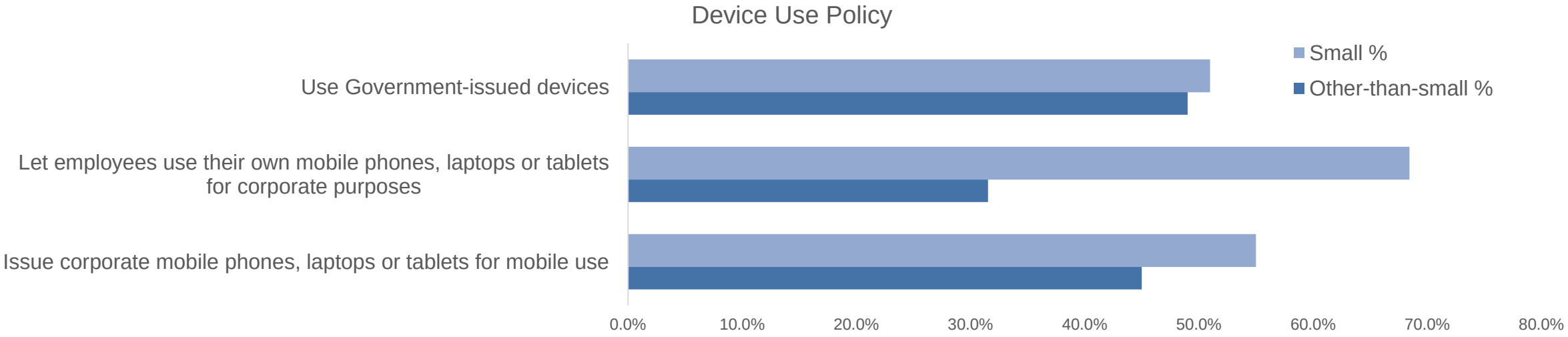
Information Technology

- **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



Information Technology

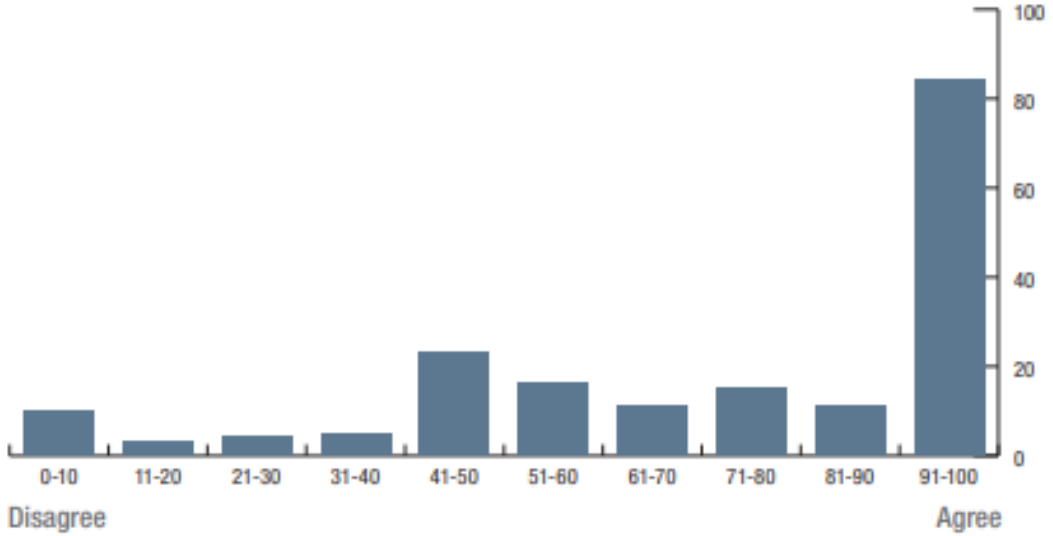


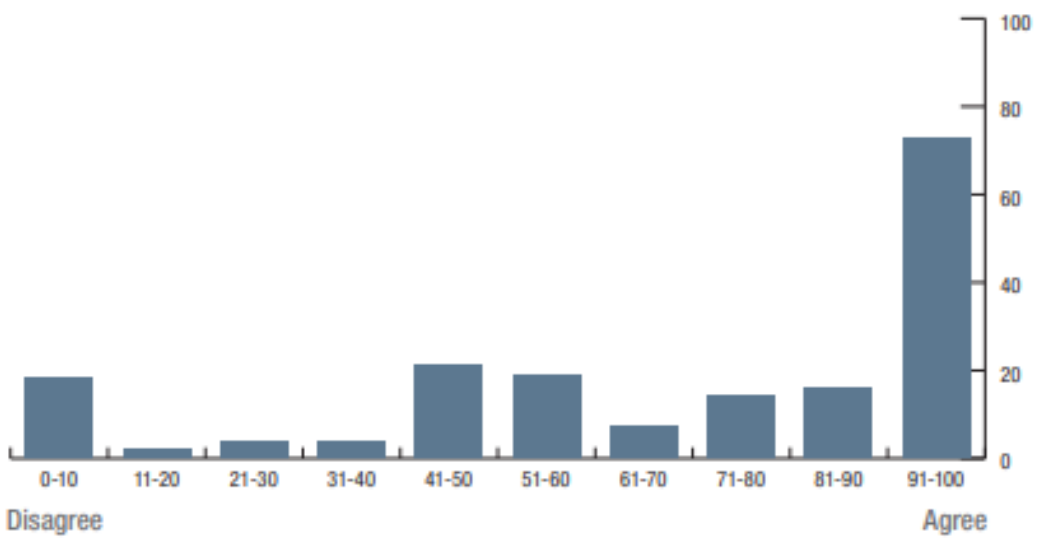


COST ESTIMATING AND ACCOUNTING

- **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

COST ESTIMATING AND ACCOUNTING



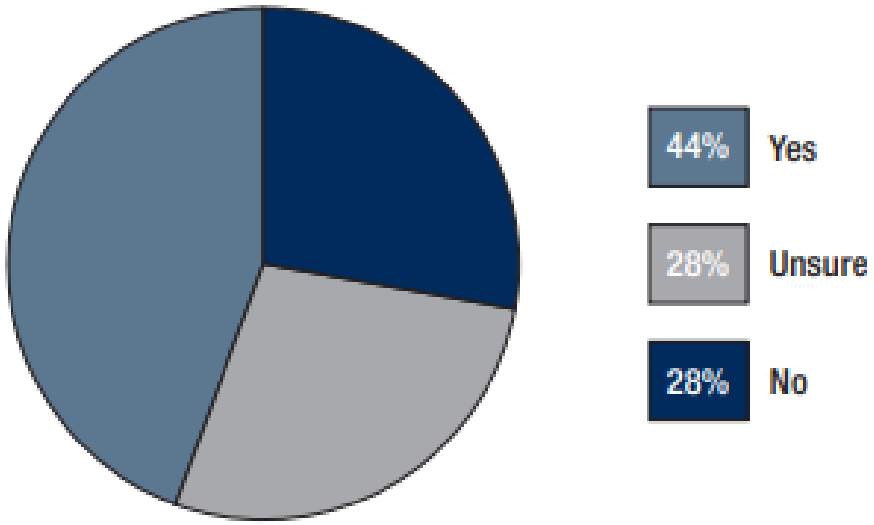


Corporate Opinions

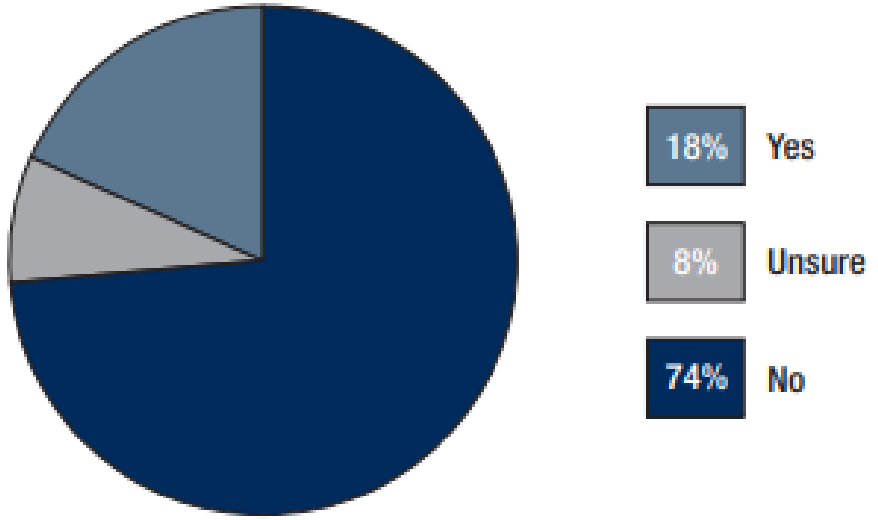
- **Key Takeaways**
  - 44 percent of companies with greater than 500 employees have been the victim of a cyber attack
  - Of a list of potential cyber-related threats, respondents are least concerned about having a contract rescinded by a prime contractor or contracting officer as a result of a cyber 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?



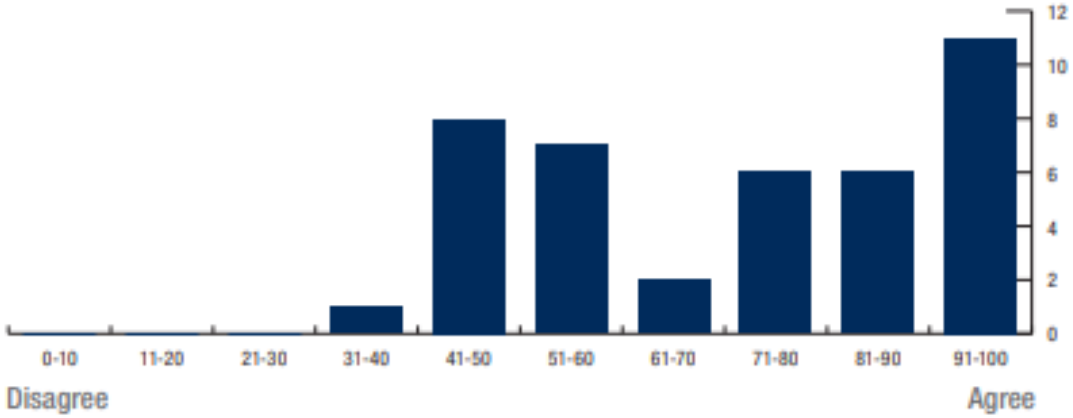
Other Than Small Business



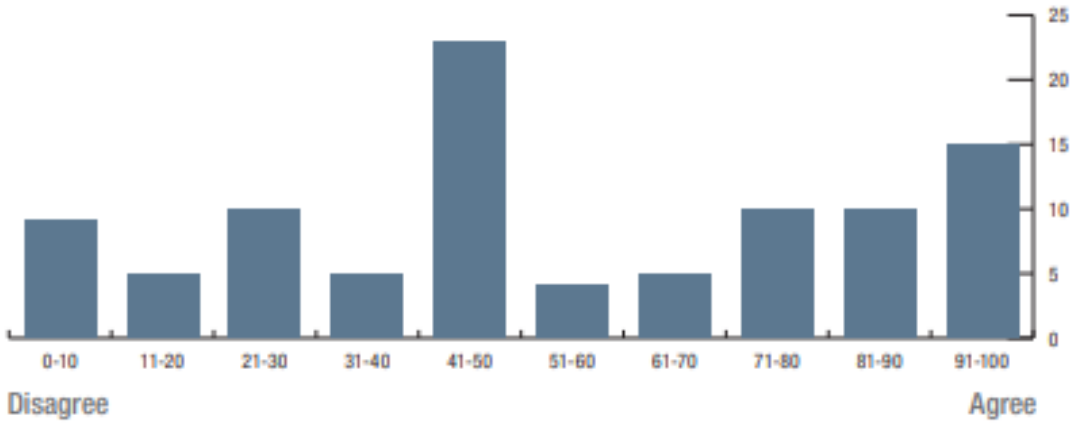
Small Business

Corporate Opinions

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



Other Than Small Business

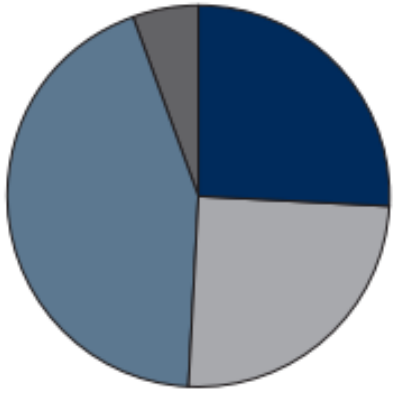


Small Business

Corporate Opinions

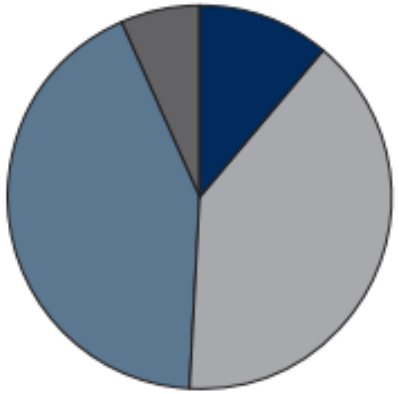
COMPLIANCE WITH DFARS 7012

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



- 5% — No, and we have taken corrective action against the subcontractor
- 44% — No, we do not currently have a documented System Security Plan (SSP) from the subcontractor
- 25% — We have requested an SSP from the subcontractor
- 26% — Yes, we have a documented SSP from 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% — Not at all – we do not handle controlled unclassified information (CUI)
- 43% — No – we saw it as a flow-down in our subcontract
- 40% — Yes – our prime(s) made us aware of the requirement
- 11% — Definitely – our prime(s) has (have) provided information on how to comply and has (have) accessible for questions and discussion

Corporate Opinions

USE OF CYBERSECURITY EDUCATIONAL RESOURCES

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.

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