San Diego Small Business Task Force

National Defense Industrial Association

NIST 800-171/DFARS 252-204.7012 Compliance

and the

DoD's Small Business Base

September, 2019

DoD's NIST 800-171 and DFARS 252-204.7012 Impacts on Small Business: Issues and Key Recommendations

San Diego Chapter of the National Defense Industrial Association
NIST 800-171 Small Business Task Force

Paper Contributors

Chris Newborn	Defense Acquisition University
Paul Shaw	Defense Acquisition University
Trenelle Lyiscott	Cytellix, Division of IMRI, Inc.
Brian Berger	Cytellix, Division of IMRI, Inc.
Ian Corey	Northrup Grumman, Inc.
Aaron S. Ralph	Pillsbury Winthrop Shaw Pittman, LLP
Larisa Breton	FullCircle Communications, LLC
Tony Lopez	INDUS Technology, Inc.

Task Force Members

Eileen Sanchez	California Governor's Office of Planning and Research
Jerome Penna	Cytellix, Division of IMRI
Trenelle Lyiscott	Cytellix, Division of IMRI
Chris Buthe	California Manufacturer Technology Consulting
Jeffrey Rude	California Manufacturer Technology Consulting
Chris Newborn	Defense Acquisition University
Paul Shaw	Defense Acquisition University
David Shaw	Get Engineering
Larisa Breton	FullCircle Communications, LLC
Jim Lasswell	INDUS Technology, Inc.
Menie Lee	INDUS Technology, Inc
Tony Lopez	INDUS Technology, Inc
Ian Corey	Northrup Grumman, Inc.
Aaron S. Ralph	Pillsbury Winthrop Shaw Pittman LLP
Brian Cruise	Pillsbury Winthrop Shaw Pittman LLP
Todd Moore	Titanium Cobra
Mike Oliver	171 Comply
Ray Moberly, Ph.D.	Faster Logic, LLC

Acknowledgements

The Task Force and Contributing Authors wish to acknowledge, with thanks, the following individuals:

Richard Jones
Brett Householder
Daryl Haegley
Members of the San Diego Small Business Committee

Each of you provided valuable experience, knowledge, insight, and advisory that enriched this project. Further, we wish to thank our colleagues at NDIA Headquarters: Wesley Hallman, Corbin Evans, Christopher Smith, and the entire policy staff for your collaboration and insights.

Table of Contents

DoD's NIST 800-171 and DFARS 252-204.7012 Impacts on Small Business: Issues and Key Recommendations

Executive Summary

Background: Since the 2016 'soft' implementation of the Defense Acquisition Regulations 252-204.7012 (DFARS 7012) requiring Defense contractors to enact reasonable security controls that include adherence to the National Institute of Standards and Technology's Special Publication 800-171 control families (SP 800-171), significant confusion and significant concern have existed in equal measure in both the Defense Industrial Base (DIB) and the Department of Defense's sub-agencies, components and commands responsible for implementing the regulations. The confusion and concern occur within the wider theatre of conflict, in which the United States has been in a largely-unacknowledged – but extremely consequential -- low intensity cyber conflict with state actors, virtual nonstate actors, and criminal actors [CC], [EE], [GG], [MM]. Intended audiences include: U.S. Policymakers, legislators, contracting corps, academy, FFRDC, QUANGO, NATO.

Scope of Study: Motivated to address and surface the discourse in the DIB, the San Diego chapter of the National Defense Industrial Association (NDIA) commissioned a Small Business Task Force (TF) which met 2018-2019. The TF work included performing literature review, soliciting anecdotal practitioner / operational experience, socialization/review by a component Command, and initiating and analyzing results from a national survey fielded in partnership with the national NDIA's policy leadership. The scope of this publication is intentionally operational as we believe the follow-on to the excellent, systemic and policy examinations already published (the 'what') should be followed up by an examination of implementation (the 'how').

Summary: The Task Force's conclusions and recommendations focus on the challenges, consequences, and impacts to small businesses of less than 50 employees, with emphasis on those small businesses of less than 20 employees, with occasional note of those micro-small businesses of 1-5 employees. Survey results from a n=285 sample provide data validating TF and wider industry observations [PP]. We focused on eight critical dimensions of DIB cybersecurity readiness, and present these in brief summary with concomitant survey measures, below. Next, we provide eight recommendations for current and future actions. Generally, this paper strongly encourages policymakers and their advisors to:

- Remember that small businesses:

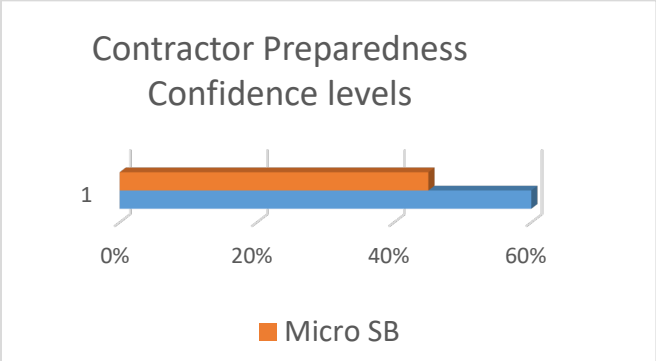
  a) form the preponderance of the body of the DIB;
  b) drive significant manufacturing revenue and employment numbers to which elected officials will be responsive; and
  c) may unintentionally create attack vectors exposing opportunities for asymmetric effects within the defense foundation of the United States.

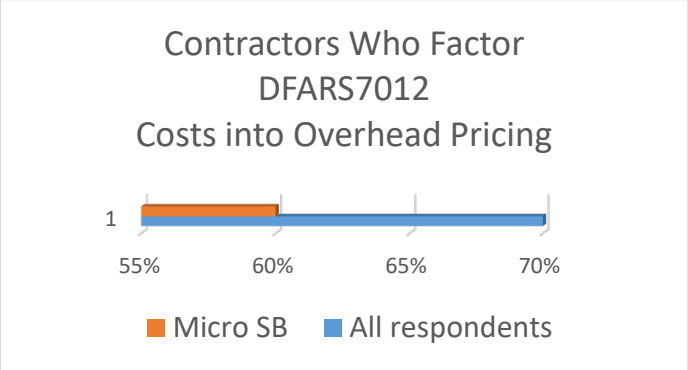
- Use market assumptions that are predicated on the extant experiences of small business, without which terminal inequities may be created, creating a contributing condition to capability loss impacting Homeland security.

- Include small businesses (those with 20 or fewer full time employees) as well as micro-small businesses (those with 5 or fewer full time employees) from all regions of the United States in pre-policy intake and policy-setting activities.

Eight critical dimensions:

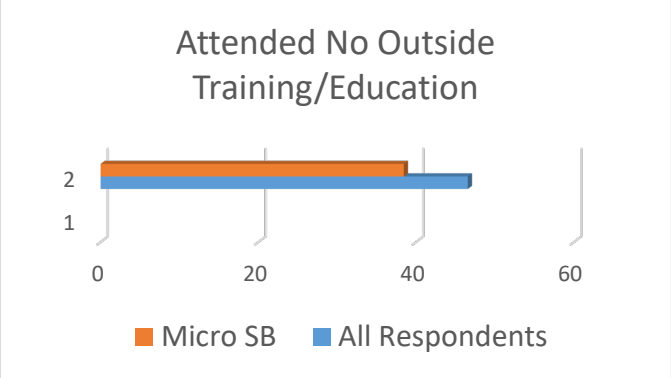
1. **Preparedness.** The degree of preparedness and understanding of what constitutes Covered Defense Information (CDI)/Covered Unclassified Information (CUI).

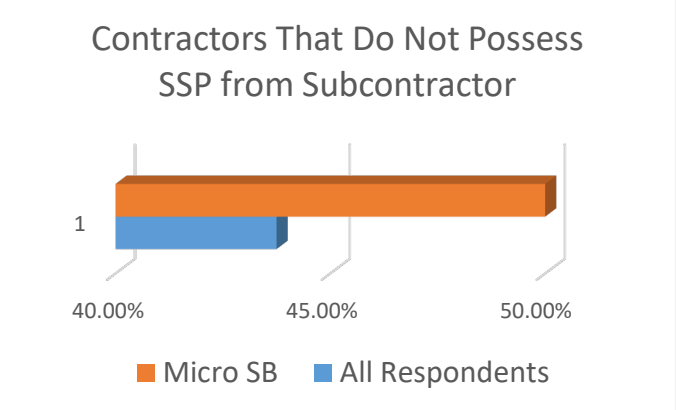




2. **Costs.** The costs of implementation, how to fold these into pricing strategies and reimbursement, and the deficiencies in financial and technical resources (otherwise known as operational and technical debt) to manage cyber security risks to meet the requirements

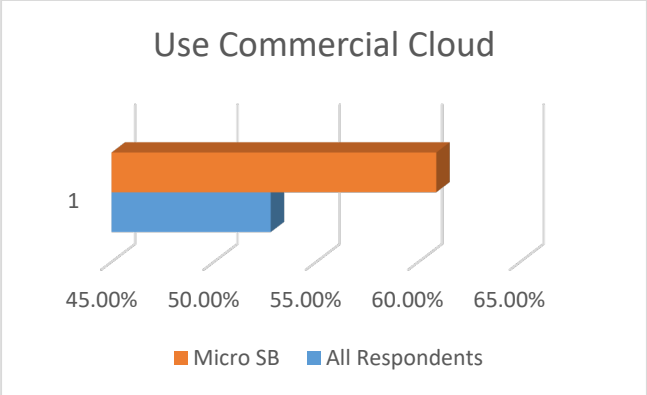
3. **Education.** How to provide continuing education to augment small business security knowledge.

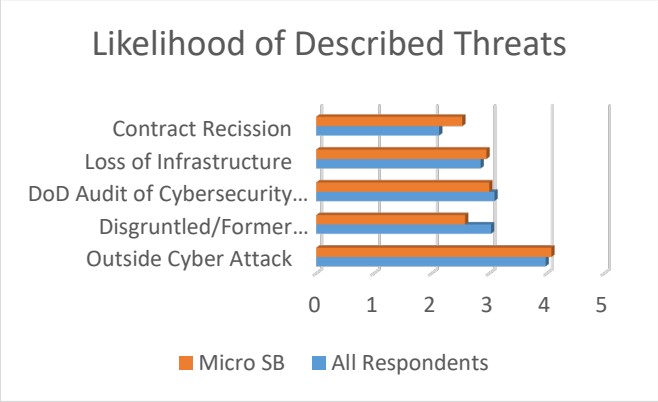




4. **Contracting**. Strategies for dealing with flow down of security requirements to subcontractors and vendors

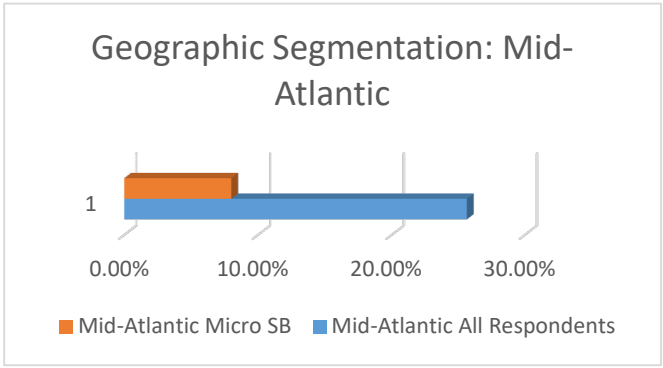
5. Cloud Computing. The degree of dependence on, and understanding of cloud computing, and small business' understanding of the additional requirements to secure information in the cloud.

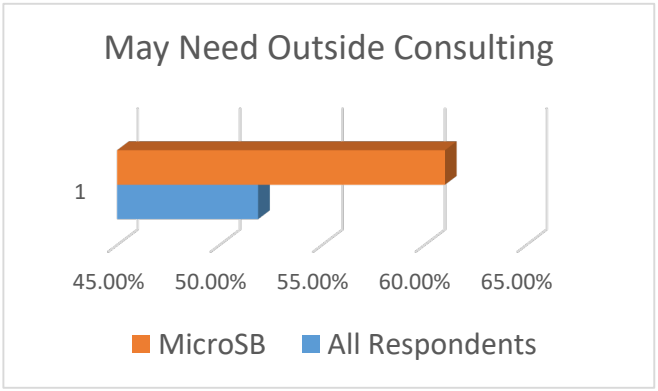




6. Risk Assessment and Remediation. The adequacy of approaches to cybersecurity risk and the adequacy of Cybersecurity defenses in place.

7. Saturation for Compliance. Methods for increasing small business awareness of the requirements of the DFARS 252.204-7012 and NIST SP 800-171 requirements at all levels





8. Certifications. Establishment of certifications for vendors providing implementation and SSP-related services to small business (not to be confused with CMMC audit certification of contractors

Recommendations in brief: The San Diego TF makes 8 recommendations around the eight dimensions of DIB cybersecurity readiness. Some are applicable to policymakers; some to Prime (large) contractors; and some to the entire diaspora for sensemaking and elaboration in future policy products. The recommendations are elaborated in subsequent introductory section and also paired with each relevant critical dimension in the body of the paper.

RECOMMENDATION #1: *Consideration must be given to the constitution of, and qualifications for, the Department's newly-introduced CMMC regimen which will involve third-party review of a contractor's security posture. As such, there is need for DoD clarification on how self-attestation will be measured; adopted; or phased-out.*

RECOMMENDATION #2: *Access to training and expertise at no additional expense must be provided in order to ensure that these companies are able to meet compliance to the standards imposed by CMMC. In addition, a compensatory pricing strategy via contracts needs to be developed in accordance with DoD's stated intent to allow direct contract reimbursement for cybersecurity.*

RECOMMENDATION #3: *Prime contractors must add a clause flowing down the 252.204-7012 requirements on their subcontract documents. These documents must state detail the specific requirements of the DFARS, to include marking, and whether or not any prospective contracted activities will include such marked CUI.*

RECOMMENDATION #4: *The requirements flowdown becomes difficult in cases where subcontractors are micro-small-business entities, which consist of 1 to 5 employees. Typically, they may be consultants one or two-person businesses. In these particular cases, the cost of compliance can be a terminal burden to the businesses, as they are often neither knowledgeable about the requirements nor do they have the technical skills to meet them. Guidance must be provided to these types of Small Businesses to ensure that they know and understand the requirements, and are able to comply without going out of business. It is imperative that additional avenues be established to expand the training of small businesses both in the service and in the manufacturing sectors. The Government needs to continue to take an active role and expand its efforts to help to educate and train small businesses. Only a tiny fraction of all DoD contractors has taken training provided by NIST MEP, Defense Acquisition University, the DoD-funded Procurement Technical Assistance Centers, and others such as California's CASCADE and Propel.*

RECOMMENDATION #5: *Ultimately, the issue of using cloud computing to meet the standards is extremely complex and may present a terminal inequity to smaller businesses. Successful use of commercial cloud computing environments by DoD contractors for sensitive information requires the successful integration of DFARS clauses 252.239-7010* and *DFARS 252.204-7012*

RECOMMENDATION #6*: Encourage uniformity in Government and corporate approach to determining security standards and individual corporate security postures. Fairly allocate responsibility for risk-reduction to all parties involved in data transit.*

RECOMMENDATION #7: *The Task Force recommends that DoD provide clear guidelines and certifications for service providers who offer DFARS 252.204-7012/NIST SP 800-171 implementation and/or auditing services within the recently-announced CMMC regimen.*

RECOMMENDATION #8: *After an evaluation and analysis with the assistance of a SWOT, the Task Force recommends expanding the approach used by the Department of the Navy (DoN) to the entire DoD. This option helps to best enable the DoD vision for shared responsibility between DoD and their contractors, especially small DoD contractors, as part of DoD's Mission Assurance and deterrence constructs.*

DoD's NIST 800-171 and DFARS 252-204.7012 Impacts on Small Business: Issues and Key Recommendations

I. INTRODUCTION

The loss of sensitive Department of Defense (DoD) information from DoD contractors is a critical threat to our national security. Sensitive DoD information includes both classified and unclassified information and resides on information technology systems controlled and operated by both federal agencies and government contractors. In the wake of recent attacks on contractor systems, the DoD implemented Defense Federal Acquisition Regulations Supplement (DFARS) clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. This clause requires contractors to implement "adequate security" to protect "covered defense information" and imposes stringent incident response obligations. To comply, contractors must establish a security posture by adhering to specified standards in National Institute for Standards and Technology (NIST) Special Publications (SP) 800-171. Contractors also must develop a system security plan, have a plan of action and milestones and to satisfy certain incident response obligations.

Small contractors struggle with the ambiguity of the requirements, as well as the cost of implementing and maintaining the required security requirements, and their accompanying security controls [EE]. In response to concerns about small business' ability to comply with these new cybersecurity requirements, the San Diego Chapter of the National Defense Industrial Association (NDIA) established a Task Force in November 2018 to study of the impact and the critical issues faced by the Small Business community in meeting these requirements. Because the Defense Industrial Base (DIB) is diverse, the Task Force sought to study the impact of the requirements on several types of DOD small business contractors (manufacturers, service providers and vendors providing assessment services). While the Task Force was comprised primarily of NDIA member organization representatives in the San Diego area, the implications of the Task Force's work have the potential to be far reaching and may be representative of the national Defense Industrial Base. Indeed, the Task Force conducted a survey encompassing both local and national NDIA members to gather data that could inform the Task Force's study of this issue. The results of that survey are detailed further in the body of this paper. At the time of writing and publication, the Task Force has included what is currently known about the emergent, mandatory Cybersecurity Maturity Model Certification requirements found at https://www.acq.osd.mil/cmmc/index.html[1]. Through this process, the Task Force makes the following recommendations:

II. SUMMARY OF RECOMMENDATIONS 1-8:

RECOMMENDATION #1: *Consideration must be given to the constitution of, and qualifications for, the Department's newly-introduced CMMC regimen which will involve third-party review of a contractor's security posture. As such, there is need for DoD clarification on how self-attestation will be measured; adopted; or phased-out.*

RECOMMENDATION #2: *Access to training and expertise at no additional expense must be provided in order to ensure that these companies are able to meet compliance to the standards imposed by CMMC. In addition, a compensatory pricing strategy via contracts needs to be developed in accordance with DoD's stated intent to allow direct contract reimbursement for cybersecurity, so companies can cover the cost of their security investments to meet the requirements, once they are awarded a contract. We also recommend that acquisitions consider covering the cost of all bidders' cybersecurity efforts that are unique*

[1] *For example, the CMMC's 9/4/2019 version 0.4 release of maturity levels 1-5 detail includes a less-to-more-stringent requirements approach. This absorbs an initial recommendation identified by the Task Force.*

to the acquisition in order to forestall loss of competitiveness in acquisition as the cost of bidding may become prohibitive within SB communities.

RECOMMENDATION #3: *Prime contractors must add a clause flowing down the 252.204-7012 requirements on their subcontract documents. These documents must state specifically and in detailed the specific requirements of the DFARS, to include marking, and whether or not any prospective contracted activities will include such marked CUI. This includes the mandate for subcontractors to:*

- *Create a Systems Security Plan (SSP) and associated plan of action and milestones (POA&Ms).*
- *Fully implement the DFARS 252.204-7014 requirements outlined in the clause and NIST SP 800-171.*
- *Report non-compliance to the DoD Chief Information Officer's (CIO)s office within 30 days after contract award.*
- *Report cyber incidents within 72 hours.*
- *Formally flow down the DFARS 52.204-7012 to all lower-tier suppliers/subcontractors storing, processing, and/or generating CDI.*
- *Be in full compliance with DFARS 52.204-7012.*

We further recommend that, along with these flow-down provisions, Prime contractors provide a contract kickoff briefing about these requirements to include training specific to the marked CUI, and list of resources, similar to those provided when handling Classified information. When establishing its contracting relationship, the Prime has the opportunity to explore marking practices and communications practices with their functional customer to reduce the footprint of any CDI to its contracting chain.

RECOMMENDATION #4: *The flow down of requirements becomes difficult in cases where subcontractors are micro-small-business entities, which consist of less than 20 employees. Typically, they may be consultants one or two-person businesses. In these particular cases, the cost of compliance can be a terminal burden to the businesses, as they are often not knowledgeable about the requirements nor do they have the technical skills to meet them. Guidance must be provided to these types of Small Businesses to ensure that they know and understand the requirements, and are able to comply without going out of business. The DoD needs more direct input from very small businesses via dialogue in Program Offices, input to policymakers, and inclusion of small business SMEs in DoD and NIST working groups and other fora. It is important to note that the small businesses closest to the Pentagon tend to be more sophisticated in cybersecurity, potentially creating a misleading perception to DoD that the entire DIB is similar. DoD outreach should include Base Community Councils, as well as the manufacturing, healthcare, FFRDC and education sectors.*

It is imperative that additional avenues be established to expand the training of small businesses both in the service and in the manufacturing sectors. The Government needs to continue to take an active role and expand its efforts to help to educate and train small businesses. Only a tiny fraction of all DoD contractors have taken training provided by NIST MEP, Defense Acquisition University, and the DoD-funded Procurement Technical Assistance Centers. We believe a significant portion of the Defense Industrial Base (DIB) may still be unaware that the requirements apply to them.

RECOMMENDATION #5: *Ultimately, the issue of using cloud computing to meet the standards is extremely complex and may present a terminal inequity to smaller businesses. Successful use of commercial cloud computing environments by DoD contractors for sensitive information requires the successful integration of DFARS clauses 252.239-7010* and *DFARS 252.204-7012.*

RECOMMENDATION #6*: Encourage uniformity in Government and corporate approach to determining security standards and individual corporate security postures. Fairly allocate responsibility for risk-reduction to all parties involved in data transit.*

RECOMMENDATION #7: *The Task Force recommends that DoD provide clear guidelines for service providers who offer DFARS 252.204-7012/NIST SP 800-171 implementation and/or auditing services within the recently-announced CMMC regimen*[2]*.*

RECOMMENDATION #8: *After an evaluation and analysis with the assistance of a SWOT, the Task Force recommends expanding the approach used by the Department of the Navy (DoN) to the entire DoD [20]. While this option will require more work on the part of DoD Program Offices, it is the best option to promote ongoing evaluation and monitoring because it is comprehensive. We believe the DoN approach also serves the useful function of stimulating dialogue between Program Offices and Contracting Officers particularly during pre-procurement activities. This option helps to best enable the DoD vision for shared responsibility between DoD and their contractors, especially small DoD contractors, as part of DoD's Mission Assurance and deterrence constructs.*

III. SUMMARY OF SURVEY RESULTS

AIMS AND METHODOLOGY. To augment and validate the Task Force's practice- and research-based observations, the Task Force developed and fielded a survey instrument in cooperation with the National Defense Industrial Association's policy department. The 35-question survey, composed of multiple choice, Likert scale, and open-ended questions, was fielded online during the first quarter of 2019 and garnered 285 total responses. The survey was fielded in accordance with best practices for market research which included: respondent anonymity, the ability for respondents to skip questions, to discontinue survey participation if desired, and to contact survey principal investigators if desired.

SURVEY RESULTS. Survey results validated practice-based observations and research assumptions by Task Force members (small business management, State industrial representatives, NIST industrial representatives, and professors specialized in secure systems engineering and acquisition). The survey results topline analysis, attached as Appendix A, as well as additional analysis filtered by Micro-Small business responses, attached as Appendix B, discovers significant differences between: Large businesses (LB), defined as businesses with 50+ employees, Small businesses (SB), defined as businesses with 20+ employees, and Micro-Small businesses (MSB), defined as businesses with 0-20 employees, with occasional emphasis on businesses with 1-5 employees. These quantified deltas center around contractor awareness (saturation); contractor technical competency; contractor readiness; contractor costs; contractor education; and contractor attitudes. Survey results are integrated into each of the eight critical domains presented in subsequent section.

[2] *We acknowledge that DoD cannot endorse specific vendors. We also note that in DFARS Case 2013-D018, DoD stated that it would not "give any credence to 3rd party assessments or certifications" regarding compliance with NIST SP 800-171. With a DoD certification program in place, however, businesses could still hire any service provider they chose, but the ability to hire a certified service provider -- while not a panacea for compliance requirements -- would provide some level of confidence in the services received.*

IV. PURPOSE OF THIS PAPER

A presidential report published September 2018 highlighted the need to improve small business contractors' cybersecurity capabilities [1], stating:

> *"Of the approximately 347,000 manufacturers in the United States, 99% are small and medium-sized manufacturers, yet more than 50% lack basic cyber controls. An assessment by Bureau of Industry and Security illustrated the cybersecurity vulnerability of small manufacturers. The survey of over 9,000 "classified contract facilities" documented that 6,650 small facilities lagged medium and large firms across a broad range of 20 cybersecurity measures. It also found that fewer than half of the small firms had cybersecurity measures in place."*

Although this presidential report focused primarily on small and medium-sized manufacturers to the exclusion of small and medium-sized service providers, its findings – if accurate – are alarming. If more than 50% of small and medium-sized manufacturers lack basic cyber controls, then more than 50% of these manufacturers necessarily lack the security measures required to protect sensitive information and to meet the NIST requirements.

More recently, in March 2019, the U.S. Department of the Navy (DON) published its own independent Cybersecurity Readiness Review (DON CRR) [CC] which identified gap DIMENSIONs in DON cyber security readiness, which includes not considering its contracting base an integral part of its systemic considerations. "The traditional distinctions between civilian and military lose meaning" when considering cybersecurity, "because defeat in one jeopardizes the other." [CC] In addition, because such businesses comprise such a large portion of the DoD contractor population, the potential for loss of sensitive DoD information represents a threat to our national security that should be addressed without delay. However, when addressing this threat, it is necessary to avoid crippling the very businesses that our nation relies on to help the DoD meet its mission and generate jobs.

Some of the compliance challenges the DIB faces result from the Government's failure to consider the structure and capabilities of small business contractors. For example, while the September 2018 presidential report acknowledges a widespread lack of basic cyber controls, the NIST Requirements upon which DFARS 252.204-7012 is based "assumes that small manufacturers currently have IT infrastructures in place, and it is not necessary to develop or acquire new systems to handle Covered Unclassified Information (CUI) [2]. In stark contrast to the reality identified by the presidential report, NIST assumes that "most small manufacturers have security measures to protect their information which may also satisfy the 800-171 security requirements." [2] Additionally, with the exception of one Request for Information (RFI) published in late 2018 by a seasoned cybersecurity program manager in DoD's Office of Energy, Installations and Environment, the DoD published no surveys, nor are we aware of any formal outreach to the Defense Industrial Base (DIB) in which upstream technical, preparedness, or economic information was sought that would support the basic assumptions made by NIST about DIB IT infrastructures.

This White Paper seeks to provide another lens through which small-business readiness can be assessed. As explained below, the organizations responsible for developing, mandating, and implementing the standards do not appear to appreciate the true impact to the DIB generally and to small business specifically. Why is this important? Because of the operational knowledge in its personnel and because of the data and systems shared between DoD and its industrial base, the DIB is an interdependent part of the

complex system [12] that makes up the United States' Homeland defense. As such, terminal impacts to the DIB should be considered as a potential root cause in a complex systems failure. [12]

> *…an exclusively internally focused-strategy is a losing one. To successfully operate in the new digital future, organizations need to look at cybersecurity within the broader multi-stakeholder environment in which they operate. Business leaders must understand themselves as key players in a dynamic and powerful ecosystem – and successful investment in the cybersecurity of this ecosystem will be the most effective defense. [LL]*

Therefore, our intent is to provide perspective into the challenges DFARS 252.204-7012 requirements impose on small businesses. As MITRE SVP William LaPlante testified in March 2019 to the Cybersecurity Subcommittee of The Senate Armed Services Committee, "While even the largest defense contractors have been victimized by the predatory cyber operations of our adversaries, the problem has been most acutely realized at the lower tiers of the defense industrial base, typically comprised of small- to medium-sized companies." [QQ] These challenges include:

- resource burden;
- technical debt; and
- operational debt

The NIST Handbook, as published, assumed that all small businesses already had some security measures in place. It is easy to see how the multitude of these businesses, which traditionally have lacked basic cyber controls, will have difficulty meeting the requirements imposed through DFARS 252.204-7012. What may be less obvious is how most small business contractors – including those with basic cyber controls – will have difficulty satisfying their contractual obligations under the new DFARS 252.204-7012 clause. As explained below, most small business contractors will encounter significant compliance challenges. Moreover, these challenges will be exacerbated because material discrepancies exist between how different government bodies apply the NIST requirements as part of the contractors' overall security posture. At the time of publication, additional confusion is occurring as DoD has announced its CMMC compliance auditing regimen even as many contractors work to finalize milestones adopted for self-attestation. The Defense Contract Management Agency (DCMA) has been tasked with audit responsibilities, and it now is adding cyber expertise to its wider mission-set.

In the interest of better understanding the impact to all sectors of the DIB, the Task Force determined that there are eight critical dimensions, which must be considered in this policy DIMENSION by DoD and by the Agencies enforcing the requirements it of NIST SP 800-171- and DFARS clause 252.204-7012 within the CMMC regimen. These critical dimensions include:

1. **Preparedness.** The degree of preparedness and understanding of what constitutes Covered Defense Information (CDI)/Covered Unclassified Information (CUI).

2. **Costs.** The costs of implementation, how to fold these into pricing strategies and reimbursement, and the deficiencies in financial and technical resources (otherwise known as operational and technical debt) to manage cyber security risks to meet the requirements.

3. **Education.** How to provide continuing education, to augment small business security knowledge. This allows small businesses to better understand on-going operations in order to detect and respond to incidents, and what is required upon detection.

4. **Contracting.** Strategies for dealing with flow down of security requirements to subcontractors and vendors:
    a. How best to segment small business sizes: 1 to 2 person consultants, to 5-20 person companies, mid to large companies, etc. This includes requirements, resources and training needed at each level. (See Recommendation One, in which we support achievable controls for smallest businesses that become more stringent with scale.)
    b. The degree of vulnerabilities through small and medium sized subcontractors with trust relationships (access) to their networks.
    c. Cost-sensitive ways for small businesses to implement security controls, including:

        1. Customer and Prime-driven strategies to reduce the need for data in motion; and
        2. Protected network enclaves similar to those used in Industrial Control System (ICS) cybersecurity – also known as PIT enclaves or FRCS enclaves.

5. **Cloud Computing.** The degree of dependence on, and understanding of cloud computing, availability of cloud service brokers/providers, availability of properly trained service auditors, and small business' understanding of the additional requirements to secure information in the cloud.

6. **Risk Assessment and Remediation.** The adequacy of approaches to cybersecurity risk and the adequacy of cybersecurity defenses in place. Key issues to address:

    a. Lack of uniform security implementation
    b. Inconsistent implementation of adequate security by defense suppliers
    c. Leveling risk on data-in-transit
    d. Reliance on self-attestation

7. **Saturation for Compliance.** Methods for increasing small business awareness of the requirements of the DFARS 252.204-7012 and NIST SP 800-171 requirements at all levels. This includes ongoing and available education (see 3, above); Prime contractor-provided training; developing an additional training corps; and directly including small businesses for representation and input into DoD and NIST working ecosystems.

8. **Certifications.** Establishment of certifications for vendors providing implementation-specific services or ongoing managed services to small business under the CMMC regimen. Establishment of a logo/seal and letter of completion/in-process that allows to the supplier/end-customer to prove they have used a qualified 3rd party provider.

To better understand the issues and impacts these critical DIMENSIONs are having on small businesses in the DIB the Task Force conducted a 35-question national survey addressing these DIMENSIONs and obtaining the first national picture, it reviewed relevant literature currently available, and it determined that small contractors typically have not created and do not understand the current security posture on their networks to adequately protect sensitive DoD information on their networks. In addition, many smaller contractors are ill equipped to shoulder the costs of implementing the security requirements in the NIST SP 800-171. They lack the in-house cybersecurity expertise necessary to implement and maintain these requirements on their own, as NIST control families call for a cross-cutting range of skills not typically found in one practitioner.

V. CRITICAL CONCERNS: DIMENSION 1: PREPAREDNESS

The degree of preparedness and understanding of what constitutes CDI/CUI.

The loss of sensitive Department of Defense (DoD) information from DoD contractors is a critical issue. This sensitive DoD information can be classified or unclassified. Smaller contractors, such as DoD manufacturers and service providers, are particularly affected with documented attacks on their intellectual property and critical information [3]. The loss of classified and controlled unclassified information has a significant effect on DoD's lethality and technological superiority [4]. "The United States cannot afford to have sensitive government information or systems inadequately secured by contractors. Federal contractors provide important services to the United States Government and must properly secure the systems through which they provide those services" [5]. Estimates on the value of annual losses of intellectual property from the United States are up to $600 billion per year [4].

Former Deputy Secretary of Defense Shanahan considered the loss of sensitive DoD information to be a critical acquisition issue and initiated a task force to address this issue [4], which has continued implementation under General Officer direction, reporting weekly to an Executive committee. The emerging DoD vision is that a shared responsibility will develop between the DoD and its contractors regarding the protection of sensitive information regardless of its location [7].

In the 2015 *Critical Manufacturing Sector-Specific Plan,* the Department of Homeland Security (DHS) identified "intellectual property theft and control system process disruption" as threats to the critical manufacturing sector [8]. Cyber-attacks by various cyber threats could affect small DoD contractors involved with manufacturing to include: loss of sensitive information; loss of control of manufacturing processes; and destruction of cyber physical systems [9] [10].

While various definitions of small DoD contractors exist, the NIST definition of a small manufacturer is one with 500 or fewer employees [11]. "Of the approximately 347,000 manufacturers in the United States, 99% are small and medium-sized manufacturers, yet more than 50% lack basic cyber controls." [12]. In many cases the smaller the organization, the less understanding it has of what constitutes CDI/CUI and the steps necessary to meet the requirements. The TF's national survey results validate these concerns. While 60% of all survey respondents indicated they were in readiness for DFARS 7012 compliance, the micro-small-business indicated a much lower level of perceived readiness – only 45%. Consultancy Sera-Brynn compiled two years of compliance assessments and found that companies are motivated to hire a consultancy to help them achieve compliance – on average, companies implemented only 39% of the NIST 800-171 controls. [PP]

VI. CRITICAL CONCERNS: DIMENSION 2: COSTS

The costs of implementation, how to fold these into pricing strategies and reimbursement, and the deficiencies in financial and technical resources to manage cyber security risks to meet the regulations.

Small contractors can struggle with the cost of implementing and maintaining the required security requirements and their accompanying security controls (Interagency Task Force, 2018). *A key issue is ensuring that CDI protection goes beyond a compliance exercise and becomes a shared responsibility between the DoD and its contractors [13].* The key is whether or not contractors can and will defend CDI on their networks from common cyber-attacks. As stated by the Defense Science Board, "while all systems should be fully defended against the most common, but less sophisticated cyber threats, it is both unaffordable and impractical to attempt to defend every system against the most sophisticated peer- level

cyber threats" *[14]. "The DoD must avoid the trap of trying to require a system to be defendable against all comers, thereby putting an ever-evolving (and un-testable) requirement onto the acquisition community and the development contractor(s)" [14]*. An important consideration-set is that resources in cybersecurity are limited, regulations are always changing, and budgets are strained especially for small businesses after years of Defense budget sequestrations. The TF national survey found a critical measure of instability in its smallest businesses that is both technical, and financial: A full 52% of MSBs indicated they utilize "DIY" IT servicing and maintenance.

DoD contractors are mandated to implement security requirements for protection of their CDI per DFARS clause 252.204-7012 [15]. Implementation of these security requirements causes small contractors to: establish a security posture; develop a system security plan; and implement incident response [16].

> *"Adequate security' means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls." [17].*

Specifically, the DoD has further defined adequate security in DFARS 252.204-7012 as implementation of 109 security requirements listed in NISTSP 800-171 R1 (Defense Federal Acquisition Regulation, 2016).

> *"DFARS clause 252.204-7012 was structured to ensure that controlled unclassified DOD information residing on a contractor's internal information system is safeguarded from cyber incidents, and that any consequences associated with the loss of this information are assessed and minimized via the cyber incident reporting and damage assessment processes." [18].*

Those implementing these security requirements will be designing their security controls to handle a moderate threat for confidentiality [16]. In NIST SP 800-171 R1, there are 110 recommended security controls to satisfy the listed 109 security requirements [16]. Additionally, NIST published a method for assessing those security controls in NIST SP 800-171A [19].

Under DFARS 252.204-7012, defense manufacturers attest to their ability to instantiate the NIST security requirements for the protection of CDI as part of their overall security approach. The Assistant Secretary of the Navy for Research, Development, and Acquisition (ASN RD&A) has modified that standard for the DoN so that the program office responsible for the contract approves the contractors' compliance with DFARS 252.204-7012 [20]. This difference means that a contractor is subject to different standards across the DoD contracting community, which also means there may be more-stringent controls imposed by an individual Program Office (PO). These additional controls may be more expensive, particularly if they are maintained only for one PO, or multiple POs drive multiple, different, requirements. While 72.58% of all survey respondents indicated they believed DFARS 7012 compliance would be a cost driver, of the smallest businesses, only 53.85% had a sense-of-cost for responding to or recovering from a cyber threat, or to say it another way, nearly half of the smallest contractors do not. More than three-quarters of all businesses surveyed (76%), though, believed that compliance costs for DARS 7012 should be directly reimbursable.

The following is a Strengths, Weakness, Opportunities, and Threats (SWOT) analysis of this security strategy issue [20]. Within the Threats section, we clearly see supply chain risk consisting of both the loss of CDI by contractors to the DoD, and loss of contractors through attrition due to their inability to absorb costs.

VII. CRITICAL CONCERNS: DIMENSION 3: EDUCATION

How to best augment Small Business security knowledge, enabling better understanding of on-going operations to detect and respond to incidents and what is required.

To meet the requirements of NIST SP 800-171 a small business must have good knowledge of their security posture and level, and of how to detect and respond to incidents should they occur. Very specific skills are required to satisfy NIST SP 800-171 security requirements. As an example, NIST SP 800-171 has nine Audit Security Requirements, which include:

- Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity
- Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions
- Review and update audited events.
- Alert in the event of an audit process failure.
- Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.
- Provide audit reduction and report generation to support on-demand analysis and reporting.
- Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
- Protect audit information and audit tools from unauthorized access, modification, and deletion.
- Limit management of audit functionality to a subset of privileged users.

An internal audit function of these nine audit security requirements requires the following:

- Monitor, analyze, investigate, and report inappropriate information system activity (Note: the internal auditor or 3rd party service provider would also need to know how to differentiate between appropriate and inappropriate system activity)
- Trace user actions (Note: the internal auditor or 3rd party service provider will require a basic knowledge of networking forensics or have tools enabled that create visualizations from log data)
- Review and update audit events (Note: the internal auditor or 3rd party service provider will require an understanding of audit events on their networks. They may need to translate corporate policy into how to make it an audited event)
- Alert on an audit process failure (Note: the internal auditor or 3rd party service provider needs a basic understanding of their corporate audit process and what activities are needed in case of an audit process failure)
- Investigate and respond to inappropriate, suspicious, or unusual activity (Note: besides the internal auditor differentiating between appropriate and inappropriate system activity, they need analysis skills to eliminate false positives on inappropriate, suspicious, or unusual activity)
- Provide on-demand analysis and reporting (Note: the internal auditor or 3rd party service provider will need an understanding of analysis and report for their corporate audit tool)
- Compare and synchronize time stamps (Note: the internal auditor will need to know how to set and monitor network time stamps)
- Protect audit records from unauthorized access, modification, and deletion (Note: this task can be done in a variety of ways. The internal auditor or 3rd party service provider should learn the basics of audit record protection)
- Limit audit functionality to privileged users (Note: the internal auditor or 3rd party service provider needs to know how to manage functionality around the audit function. There could be variance in methods for different audit tools.)

Many small businesses, especially the sub-set of MSBs with 1-5 employees, do not have the sophistication or capability to perform the functions above. While more MSBs indicated they had taken some training (61.54%) than the full survey cohort (53.48%), barely less than half of MSBs (49%) believe their employees are "well prepared to understand and respond to cybersecurity threats." They must either hire personnel with the necessary expertise, or engage the services of a company that can help them with the implementation and operational aspects. Either of these options will be an additional expense that most companies this size cannot absorb.

VIII. CRITICAL CONCERNS: DIMENSION 4: Contracting

Strategies for dealing with flow-down of security requirements to subcontractors and vendors.

NIST SP 800-171 and DFARS 252.204-7012 aim to ensure vendor compliance and validation of in-house information systems and more importantly address any cybersecurity gaps, which may lead to loss or compromise of CDI or CUI. A significant aspect of DFARS 252.204-7012 is the subcontractor flow-down requirement. This clause states all requirements must flow down to subcontractors without regard to their supply chain tier position level that store, process and/or generate CDI as part of contract performance. It is important to point out that, CUI requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies, and is:

1. Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

2. Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

It is important to note that the prime contractor holds full responsibility for ensuring compliance and is ultimately responsible for the compliance of their suppliers and subcontractors. The TF survey found, though, that Prime contractors have not received completed SSPs from their subcontractors (43.75%), and another 25% had requested a SSP with competition status unknown to the survey, with a combined additive weight of these measures indicating that 68.75% of Prime contractors are without a compliant supply chain. Prime contractors must ensure that the flow down of requirements and the validation of compliance is formally documented and can be verified.

The use of low-cost Governance, Risk, and Compliance (GRC) technology may be a solution for these organizations. Some these tools can be extended to compliance with DFARS 252.204-7012. These businesses may also:

- Partner with a Managed Security Services Partner (MSSP) that offers a compliance and reporting capability specific to NIST SP 800-171. Many of the required controls can be mapped back to managed service offerings to produce automated compliance reporting. [22]
- Work with contracting organizations to create and implement processes that can be incorporated into the existing contracting business cycle. Contracts staff already play a key role related to subcontractor compliance for other contract clauses and adding DFARS 252.204-7012 requirements should be a logical fit. [22]

Bottom-line: It's the prime contractor's obligation to flow down DFARS 252.204-7012 requirements to all suppliers or subcontractors. Fewer than 20 percent of MSBs (17.95%) surveyed say they received information about how to comply with the requirements from their primes. Planning for success now is imperative. [22]

IX. CRITICAL CONCERNS: DIMENSION 5: Risk Assessment and Mitigation

The adequacy of approaches to Cybersecurity Risk and the adequacy of Cybersecurity defenses in place.

No company, no matter the size, number of years in business, revenue, or skillsets is immune from cyberattack. Even the largest companies in the world with generous budgets cannot escape cyberattacks. Why? Hackers do not discriminate. It is not a matter of "if," but "when." Whether you are involved in government contracting, have a risk management framework as an objective, or require compliance with standards, developing a cybersecurity program is a critical best practice.

Why are defense suppliers at risk?

- Unsecured intellectual property
- Limited cyber & IT resources
- Constrained security budgets
- Constant system upgrades, moves & changes
- Ever-changing compliance requirements and policies

Inconsistent implementation of adequate security by defense suppliers:

One of the largest misconceptions of cybersecurity compliance has been the delivery of documentation and self-attestation, such as a Plan of Action & Milestones (POA&M) and the Systems Security Plan (SSP) to show compliance activity. Many organizations in the supply chain are either doing this work independently or outsourcing. Once these documents have been developed, the ownership and progress needed to meet 100% compliance becomes a low priority. There is little ownership of the POA&M which is the workflow for meeting compliance. The purpose of these documents is to show continuous improvement towards compliance and improved cyber posture, as opposed to meeting a contractual requirement.

Contractual requirements have become the driver for cyber preparedness and are slated to become the fourth pillar of DoD acquisition. The challenge arises in the competing obligations to meet contract objectives, self-attest to compliance regardless of risks while engaged in the normal course of business where other business objectives may have a much higher priority than cyber preparedness.

Organizations are taking risks, cutting corners and looking for the easiest solution. It is telling that both all respondents, and MSBs, rated a DoD cybersecurity audit as the third-highest risk to their business! To make a difference in cyber protection, more investment is required by the ecosystem. Best practices indicate that an independent 3rd party audit and assessment is necessary to produce a nonbiased cyber posture. The use of consistent 3rd party assessments, 3rd party audits, 3rd party vulnerability identification and 3rd party cyber-monitoring for attack vectors will improve the DoD's supply chain cyber posture. Without investment in the ecosystem and/or enforcement with significant damages, the supply chain will raise its cyber posture to the minimum bar. *Today, the minimum bar is a documentation exercise as opposed to actual cybersecurity preparedness.* The system is inconsistent because companies within the DIB may not know how to adequately identify and describe risk; and also because the DIB may be onboarding risk when companies enact a paper compliance regimen as opposed to an active security posture.

Lack of Uniform Security:

Lack of uniform security requirements occurs at the policy and Governmental level [BB], and it also occurs within corporate implementations. Uniformity of the standards and expected outcomes can harmonize measurement of an organization's cyber posture. For example, an assessment that relies upon a question and answer method for analyzing the 109 controls of NIST SP 800-171, only relies upon the quality of the assessor. A "yes" answer for a given control, requires that the assessor "audit through evidence" that the control is truly a "yes". Likewise, a "no" may also be audited for status, and there may be remediation activity that indicates the control is in process for compliance. In addition to the interview model, a set of tests or scans of an organization can identify vulnerabilities that are not identified in the interview. In reality, a company cannot truly identify its cyber posture without an independent 3rd party audit, scans and monitoring. And, survey respondents agreed: More than half (52%) of all survey respondents agreed they would probably need to engage outside help to bring themselves into compliance.

Cybersecurity assessments take on many forms. There are proprietary models to assess an organization based upon a set of criteria as defined by the practitioner. There are standards-based approaches across different compliance models and there are self-assessment tools available. All provide a subjective level of cyber posture for an organization. However, there are flaws in most assessment models in that they do not measure the truth about an organizations physical, logical and digital cyber posture via an organized and thorough cyber gap analysis.

An assessment should be designed to meet both compliance requirements and the objectives of "Identify, Protect, Detect, Respond and Recover" concepts. Within each category, a set of guidelines, processes, procedures, technologies, and implementation plans must be provided.

Each independent audit should indicate remediation solutions that meet or exceed compliance. For example, a recommendation stating: "Go buy Microsoft Office 365 version "xyz" that enables the NIST SP 800-171 compliance features" is poor advice and is not actual compliance. Office 365 can help an organization meet components of compliance if all the controls are enabled correctly and the controls are tested and audited.

Of additional concern is the risk shouldered by the DIB for data in transit. As previously elaborated, a determined near-peer adversary can subvert contractor controls and also subvert the data transit infrastructure in a variety of ways. We respectfully recommend that DoD lever its position to impose standards requiring safe passage at transfer points, during transfer, and at delivery, on those entities possessing the scale and resources to defend against sophisticated criminal, nation-state, or virtual nonstate actors.

X. CRITICAL CONCERNS: DIMENSION 6: Cloud Computing

The degree of dependence on, and understanding of cloud computing, availability of cloud service brokers/providers, availability of properly trained service auditors, and small business' understanding of the additional requirements to secure information in the cloud.

The use of commercial cloud computing requires a change in DoD and contractor risk management, as neither party has control of the physical infrastructure storing data and providing critical services [23]. Many organizations seem to underestimate their risk by trusting cloud service providers (CSP) and do not seem to appreciate their shared responsibility with the cloud service providers for security and resilience [23]. This has especially become the case with small businesses manufacturers and service providers, as cloud computing provides SBs and MSBs with critical operational functioning, virtual (distance) task performance, and scalability. In the full survey, 52.78% of respondents indicated they utilize CSPs – but 60.87% of MSBs surveyed indicated they use the cloud.

Sensitive DoD information and DoD critical services are increasing dependent upon the continuation of services and protection from CSPs. The use of commercial cloud environments for storage of sensitive DoD information requires a complex integration between DFARS clause 252.239-7010, Cloud Computing Services, and DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. Many smaller DoD contractors may not have successfully integrate these two DFAR clauses.

The DoD has created a cloud computing security requirements guide and a connection process guide [25]; [23]. To understand the cybersecurity expertise to the risk to mission assurance from the use of cloud capabilities, DoD also created information impact levels (IILs) [23]. A cloud service provider's IIL rating is an assessment of the impact for the loss of confidentiality, integrity, or availability of data, systems, or networks [23]. IILs apply even when contractors use commercial cloud environments to store sensitive unclassified DoD information. If defense contractors use commercial cloud services for the storage and processing of sensitive DoD information like CDI, they also trigger the provisions of DFARS 252.239-7010, Cloud Computing Services (Defense Federal Acquisition Regulation Supplement, 2016). Core requirements of DFARS 252.239-7010 include:

- "approval from the Contracting Officer prior to utilizing cloud computing services in performance of the contract;"
- "implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with the Cloud Computing Security Requirements Guide (SRG);"
- "maintain within the United States or outlying DIMENSIONs all Government data that is not physically located on DoD premises;"
- "contractor shall report all cyber incidents that are related to the cloud computing service provided under this contract." [23]

These requirements are in addition to the 109 security requirements for protecting sensitive DoD information under NIST SP 800-171 as a result of DFARS 252.204-7012. Thus, the DoD and DoD contractors require an understanding of how to use cloud services securely, even if the CSP has an excellent security posture.

There is a concern that small and medium sized DoD contractors may not have cybersecurity expertise to successfully perform the integration of the two applicable DFAR clauses. Use and protection of CSPs is still evolving in the DoD's security strategy. The issue is to ensure continuity of CSP services and secure sensitive information at the CSP from advanced cyber threats.

The current strategy for cloud cyberspace protection is based on collaboration between the DoD and a CSP to achieve situational awareness [26]. It allows the DoD to limit potential effects from a compromised CSP to the DoD Information Network (DoDIN) by controlling accesses and services at a cloud access point [26]. Critical infrastructure service providers, like a CSP, are responsible for: fighting through the cyber-attack; maintaining continuity of operations; and determining when to request assistance from the government [27]. There is still an evolving standard for when government assistance will occur in any security and resilience efforts in response to a cyber-attack on commercial assets. This strategy has created a vulnerability to the defense of critical infrastructure. [5]; [RR] (2018 National Cyber Strategy and the 2018 DoD Cyber Strategy. Additionally, Executive Order 13800, strengthening the Cybersecurity of Federal Networks and Critical Infrastructure of has sought ways for government agencies to employ and support the cybersecurity capabilities of critical infrastructure [SS]. Both the 2018 National Cyber Strategy and the 2018 DoD Cyber Strategy increase the role of government for cyber defensive and offensive operations to protect critical infrastructure, to include that which is commercially owned and operated [5]; [7].

The loss or impairment of commercial CSPs by highly capable state-sponsored cyber threat actors is a critical issue. The DoD is evolving the ability to counter a significant and capable state-sponsored cyber threat to commercial cloud service providers as part of the U.S. critical infrastructure. The DoD envisions a shared responsibility between DoD and their commercial critical infrastructure service providers, especially for smaller and medium sized CSPs, to include maintenance of data security and critical service continuity of operations.

A key issue is that of security and resilience against an advanced nation state threat goes beyond basic security controls and becomes a shared responsibility between the DoD and its critical infrastructure service providers [13]. Chinese and Russian state-sponsored cyber threat actors have conducted reconnaissance on U.S. critical infrastructure and are advancing their cyber-attack capabilities [TT]. Major commercial CSPs have extensive security capabilities, but there are numerous commercial CSPs with varying degrees of cybersecurity expertise [UU]. Smaller CSPs, which Gartner classifies as tier 3 providers, can struggle with the cost of implementing and maintaining recommended security capabilities [UU]; [REF]. While most CSPs should be able to defend against common cyber threats, "it is both unaffordable

and impractical to attempt to defend every system against the most sophisticated peer-level cyber threats" [14]. Commercial critical infrastructure service providers should have an expectation of assistance of security and resilience, if attacked by highly capable state-sponsored cyber threat actors [14].

XI. CRITICAL CONCERN: DIMENSION 7: SATURATION

Methods for increasing small business awareness of the requirements of the DFARS252.204-7012 and NIST SP 800-171 at all levels.

Small businesses in the DIB may benefit from greater understanding of NIST SP 800-171 and DFARS 252.204-7012, especially when it comes to understanding the framework required by law or applicable under vendor due diligence. For certain, there is much confusion within the DIB regarding the required due diligence which drives implementation of the standards. The proliferation of NIST SP 800-171 as the de facto security framework for organizations that choose to follow federal standards or for organizations doing business with the government has created some confusion in the marketplace. We do not believe that there is uniform understanding within and amidst the DIB that *all contractors are covered*. Nor do we believe, based on geographic distribution of survey responses that skewed heavily to the East and West coasts, that this understanding is saturated evenly among the different regions of the U.S.

Many organizations are receiving blanket requirements from prospective clients to align with NIST SP 800-171. These requests are often part of a vendor management checklist that does not distinguish between organization type, associated risk, or size. It is therefore critical that a strong information campaign be undertaken to expand awareness and understanding of NIST SP 800-171. To date, the NIST organization has sponsored several education briefings for industry at its headquarters in Bethesda, MD. Individual NDIA chapters have hosted volunteer SMEs to walk through the requirements. The national PTAC body, APTAC, likewise has provided training to its counsellors. The DoD CIO senior staff has travelled to visit Defense Acquisition University (DAU) and briefed California's Manufacturing Exchange Partnership.

In California, DAU is holding town hall-style training to educate the DoD contracting corps and contractors. Also, the DoD's Office of Economic Adjustment made a Propel grant to the San Diego Military Advisory Council, which is working with individual subject matter experts and San Diego's Cyber Center of Excellence (SDCCoE) to develop an informational product as part of its granting activities. The San Diego Contracting Opportunities Center (SDCOC)/Procurement Technical Assistance Center (PTAC) sponsored standing-room-only training for contractors in 2018 and the California Advanced Supply Chain Analysis & Diversification Effort (CASCADE) are is also conducting sessions to help training the small business sector. The NDIA NIST SP 800-171 Task Force and this study are part of this community outreach effort. Its aim is to frame the many issues and impact of the NIST requirements on small business, and to provide a comprehensive briefing document and a survey of the DIB to be deployed nationally in order to assess DIB readiness and provide analyzed datasets for modeling and projections. These types of outreach activities must be continued and increased to ensure saturation within the DIB.

XII. CRITICAL CONCERNS: DIMENSION 8: Certifications

Establishment of certifications for vendors providing implementation and auditing services to small business.

Most small businesses have neither the expertise nor the intrinsic resources necessary to fully implement DoD and DFARS 252.204-7012 cybersecurity requirements, and must instead rely on outside service providers for assistance. A plethora of service providers exist, promising to help businesses become compliant with DFARS 252.204-7012.

For many small businesses, the cost of engaging one or more of these service providers is not insubstantial. The quality of the services provided, however, can vary significantly from one provider to the next, and might not actually leave the customer in a position of full compliance with applicable standards. Given their lack of expertise, many small businesses are unable to make an informed choice when selecting service providers or to evaluate what they have purchased.

XIII. CONCLUSION

The above discussion leads to two different courses of action (COA):

1. Institutionalize Department of the Navy (DON) process across the DoD for program offices to approve a contractor's compliance with DFARS 252.204-7012.
2. Allow an independent third party to certify and audit contractor compliance with DFARS 252.204-7012.

Indeed, these COAs must involve more problem solving for the supply chain. To a large degree many of the issues within the supply chain are vagueness and a response to "what should be done – specifically": Assessment, Vulnerability Testing, Continuous Monitoring, updating Assessment and POA&M's as remediation's occur, continuous scanning and testing for new vulnerabilities and weaknesses, etc.

Contractors are struggling with implementation of the 109 security requirements of NIST SP 800-171 as required by DFARS 252.204-7012, as they could lack cybersecurity expertise for evaluation and monitoring of implemented security controls. The Assistant Secretary of the Navy for Research, Development, and Acquisition (ASN RD&A) implemented a different standard than COA 1 due to a concern with contractor's self-assessing their security posture [20]. COA 2 forces an increased involvement of the program office in the evaluation of a contractor security posture to protect CDI. This COA follows the shared partnership envisioned in the *National Cyber Strategy of the United States of America* (2018). COA 3 for independent third-party assessments may have issues. "Security audits are often inadequate for estimating future impact of control implementation, since cyber threats can evolve quickly, rendering one-time analyses obsolete" [28]. With a critical need for ongoing interaction between the program offices and their contractors for the protection of CDI, the Navy is implementing COA 2. COA 2 allows the DoD a better partnership opportunity to secure "DoD information and systems against malicious cyber activity, including DoD information on non-DoD-owned networks" [7].

The loss of sensitive Department of Defense (DoD) information from DoD contractors is a critical issue. Unclassified sensitive DoD information categorized as CDI has been a frequent target of foreign cyber-attacks. DoD contractors are required to develop a security posture through DFARS 252.204-7012. Small DoD contractors are struggling to implement their required security posture for CDI on their networks, with issues of cost and cybersecurity expertise. A critical issue going forward is to turn DoD contractor implementation of the DFARS clause 252.204-7012 security requirements into a shared responsibility and a partnership, instead of a compliance exercise.

The DoD vision is for a shared responsibility between the DoD and their contractors for the protection of CDI, regardless of its location. This paper explored the existing DoD option, a modified option implemented by the DoN, and the use of independent third-party assessments.

REFERENCES AND SOURCES CITED

[1] https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF) (p. 87-88) (p. 3)

[2] ”NIST Handbook 162 (NIST MEP Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements) at 3

[3] Nakashima, E., & Sonne, P. (2018). China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html?noredirect=on&utm_term=.8836302b51d5

[4] Mattis, J. (2018). *Establishment of the protecting critical technology task force.* Secretary of Defense Memorandum. Washington, D.C.

[5] Trump, J. (2018). *National cyber strategy of the United States of America.* The White House. Washington, D.C. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[6] Defense Federal Acquisition Regulation; DFARS 252.239-7010, Cloud Computing Services (2016)

[7] U.S. Department of Defense, 2018, p. 5

[8] U.S. Department of Homeland Security. (2015). *Critical manufacturing sector-specific plan an annex to the NIPP 2013.* p. 7 Retrieved from https://www.dhs.gov/sites/default/files/publications/nipp-ssp-critical-manufacturing-2015-508.pdf

[9] Ponemon Institute. (2017). *2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB).* Retrieved from https://keepersecurity.com/2017-State-Cybersecurity-Small-Medium-Businesses-SMB.html

[10] U.S. Department of Homeland Security. (2018). *Critical manufacturing sector: Sector overview.* Department of Homeland Security website. Retrieved from https://www.dhs.gov/critical-manufacturing-sector

[11] Paulsen, C., & Toth, P. (2016*). Small business information security: The fundamentals* (NISTIR 7621 Rev. 1). Bethesda, MD: National Institute of Standards & Technology (NIST). Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.7621r1.pdf

[12] Interagency Task Force. (2018). *Assessing and strengthening the manufacturing and defense industrial base and supply chain resiliency of the United States*. Report to the President. p. 87, Retrieved from https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF

[13] Nissen, W., Gronager, J., Metzger, R., & Rishikof, H. (2018). *Deliver Uncompromised: A strategy for supply chain security and resilience in response to the changing character of war.* The Mitre Corporation. McLean, VA. Retrieved from https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-8AUG2018.pdf

[14] *Defense Science Board, 2013, p. 84*

[15] DFARS clause 252.204-7012 (2016)

[16] Ross, R., Viscuso, P., Guissanie, G., Dempsey, K., & Riddle, M. (2016). *Protecting controlled unclassified information in nonfederal information systems and organizations (*Special Publication 800-171 Rev 1). National Institute of Standards and Technology. Gaithersburg, MD. Retrieved from

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

[17] Office of Management and Budget. (2016) p. 26. *Managing information as a strategic resource* (Circular A-130). Washington, D.C. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

[18] Toth, P. (2016) p. 3. *NIST MEP cybersecurity self-assessment handbook for assessing NIST SP 800-171 security requirements in response to DFARS cybersecurity requirements* (NIST Handbook 162). National Institute of Standards and Technology. Gaithersburg, MD. Retrieved from https://nvlpubs.nist.gov/nistpubs/hb/2017/nist.hb.162.pdf

[19] Ross, R., Dempsey, K., and Pillitteri, V. (2017). *Assessing security requirements for controlled unclassified information (Draft)* (Special Publication 800-171A). National Institute of Standards and Technology. Gaithersburg, MD. Retrieved from https://csrc.nist.gov/CSRC/media/Publications/sp/800-171a/draft/sp800-171A-draft.pdf

[20] Department of the Navy Memorandum (2018). *Implementation of Enhanced Security Controls on Select Defense Industrial Base Partner Networks*.

[21] *Homeland Security Science and Technology Directorate, 2018*

[22] Cybersheath 2018, https://www.cybersheath.com/2017-progress-cybersecurity-opportunity-2018/

[23] Hein, M. (2017). *Department of Defense (DoD) cloud connection process guide* (Version 2). Laurel, MD.: Defense Information Systems Agency. Retrieved from *https://www.disa.mil/Network-Services/Enterprise-Connections/Connection-Process-Guide*

[24] McAfee, LLC. (2018b). *Navigating a cloudy sky practical guidance and the state of cloud security.* Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-navigating-cloudy-sky.pdf

[25] Defense Information Systems Agency. (2017a). *Cloud computing security requirements guide* (Version 1, Release 3). Retrieved from https://iasecontent.disa.mil/cloud/SRG/index.html

[26] Defense Information Systems Agency. (2017b). *Department of Defense cloud cyberspace protection guide* (Incorporating Change 1). Retrieved from https://rmf.org/wp-content/uploads/2018/05/DOD_Cloud_Cyberspace_Protection_Guide-19DEC2017.pdf

[27] Schneider, J., Schechter, B., & Shaffer, R. (2017). *Navy – private sector critical infrastructure war game 2017 game report.* Newport, R.I.: Naval War College. Retrieved from http://www.nwcfoundation.org/Files/Admin/Corp%20Logos/Navy-Private%20Sector%20Critical%20Infrastructure%20War%20Game%20Report%20%281%29%20%282%29.pdf

[28] Homeland Security Science and Technology Directorate, p. 12, 2018

[AA] Defense Science Board. (2018). *Cyber as a Strategic Capability (including DoD Memoranda).* Retrieved from https://www.acq.osd.mil/dsb/reports/2010s/DSB_CSC_Report_ExecSumm_Final_Web.pdf

[BB] Ackerman, R. *When It Comes To Cybersecurity, the Federal Government Is Nowhere To Be Found.* July 2019. Retrieved from: https://www.cyberscoop.com/federal-government-cybersecurity-bob-ackerman/

[CC] Secretary of the Navy. *Cybersecurity Readiness Review*. (March 2019).

[DD] Department of Defense Cost Analysis on NIST SP 800-171 Compliance. (2019) Retrieved from: https://www.regulations.gov/document?D=DOD-2019-OS-0072-0001

[EE] Donnelly, J. and Ratnam, G. "Virtually Defenseless

The national security establishment is woefully unprepared for the new era of cyber-warfare." CQ Magazine (July 2019). Retrieved from:https://lrl.texas.gov/whatsNew/client/index.cfm/2019/7/11/Current-Articles--Research-Resources-July-11

[FF] Doubleday, J. “Pentagon to require new cybersecurity ‘certification’ from defense contractors.” Inside Defense (31 May 2019). Retrieved from: www.InsideDefense.com

[GG] Lubold, G. and Volz, D. “Navy under ‘Cyber Siege’ by Chinese Hackers.” The Wall Street Journal (March 2019).

[HH] Under Secretary of Defense for Acquisition and Sustainment Memorandum. Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review (January 2019).

[II] Under Secretary of Defense for Acquisition and Sustainment Memorandum. Strategically Implementing Cybersecurity Contract Clauses (February 2019).

[JJ] Defense Contracting Management Agency. Strategically Implementing Cybersecurity Contract Clauses Handbook amendment (February 26, 2019).

[KK] DoD Office of Energy, Installation and Environment Request for Information WHSOSBP-EATL-001, Cybersecurity Costs – General. (2019)

[LL] Dixon, W. and Lewis, R. *The smartest cyber investment is collective action. Here’s why.* World Economic Forum newsletter (July 18, 2019). Retrieved from www.weforum.org

[MM] Breton, L. *Virtual NonState Actors as Clausewitzian Centers of Gravity*. Leading Issues in Cyber Warfare and Security, J.C.H. Ryan, ed. (pp. 107-117, 2015).

[NN] Cook, R. *How Complex Systems Fail*. (Cognitive Technology Laboratories, University of Chicago,
1998.) Retrieved from: https://web.mit.edu/2.75/resources/random/HowComplexSystemsFail.pdf

[OO] Doubleday, J. “New Report Finds Defense Contractors Struggling with Cybersecurity,” Inside Defense, May 21, 2019. Retrieved from: https://insidedefense.com/daily-news/new-report-finds-defense-contractors-struggling-cybersecurity-requirements

[PP] “Reality Check: Defense industry’s implementation of NIST SP 800-171” SeraBrynn Consultancy monograph, May 2019. Retrieved from:

[QQ] Testimony of Dr. William LaPlante before the Cybersecurity Subcommittee of The Senate Armed Services Committee, March 2019. Retrieved from:

[RR] U.S. Department of Defense. (2018). *Fact sheet: 2018 DoD cyber strategy and cyber posture review.* Retrieved from https://media.defense.gov/2018/Sep/18/2002041659/-1/-1/1/Factsheet_for_Strategy_and_CPR_FINAL.pdf

[SS] Trump, J. (2017). Executive Oder (EO)13800 Issue 1. The White House. Washington, D.C. Retrieved from ttps://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

[TT] Coates, D. (2018). Worldwide threat assessment of the U.S. intelligence community. Washington, D.C.: Director, National Intelligence (DNI). Retrieved from https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

[UU] Helser, J. (2017). How to evaluate cloud service provider security. Gartner Report ID G00340272. Retrieved from https://www.gartner.com/doc/3833968?refval=&pcp=mpe

GLOSSARY

ASN RD&A	Assistant Secretary of the Navy for Research, Development and Acquisition
CCoE	Cybersecurity Center of Excellence (San Diego)
CMMC	Cybersecurity Maturity Model Certification
COA	Course of Action
CSP	Cloud Service Provider
CUI	Controlled Unclassified Information
CDI	Covered Defense Information
DFARS	Defense Federal Acquisition Regulations
DIB	Defense Industrial Base
DOD	Department of Defense
DON	Department of the Navy
DODIN	Department of Defense Information Networks
IILs	Information Impact Levels
MA	Mission Assurance
MEP	Manufacturing Exchange Partnership
MSB	Micro-Small Business
NDIA	National Defense Industrial Association
NIST	National Institute of Standards and Technology
NARA	National Archives Registry
PO	Program Office
PTAC	Procurement Technical Assistance Center
RM	Risk Mitigation
RMF	Risk Management Framework
SB	Small Business
SOP	Standard Operating Procedure
SP	Special Publication
SWOT	Strengths, Weaknesses, Opportunities and Threats
TF	Task Force
TTP	Tactics, Tools and Procedures

APPENDIX A

DoD's NIST 800-171 and DFARS 252-204.7012 Impacts on Small Business:
Survey Results Topline Analysis

NDIA 2019 CYBERSECURITY SURVEY RESULTS SUMMARY

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.

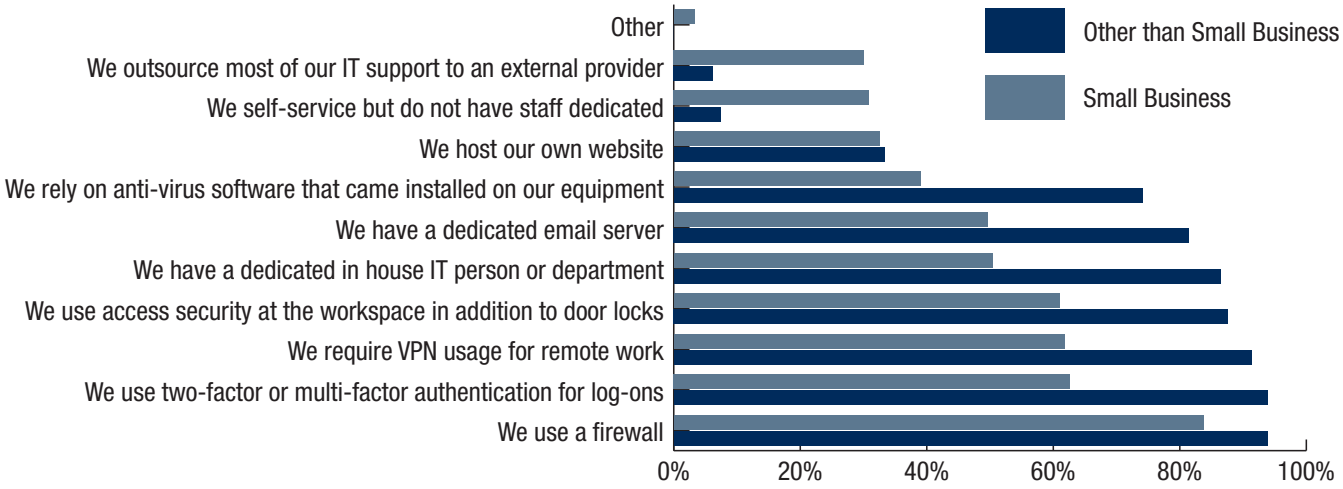
KEY TAKEAWAYS

- 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

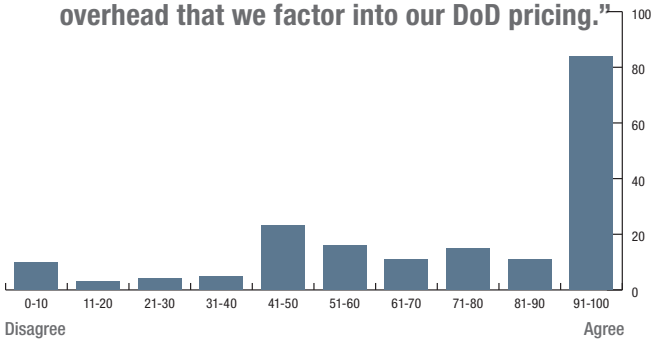
TOP THREE BIGGEST CYBER THREATS FACING INDUSTRY:

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

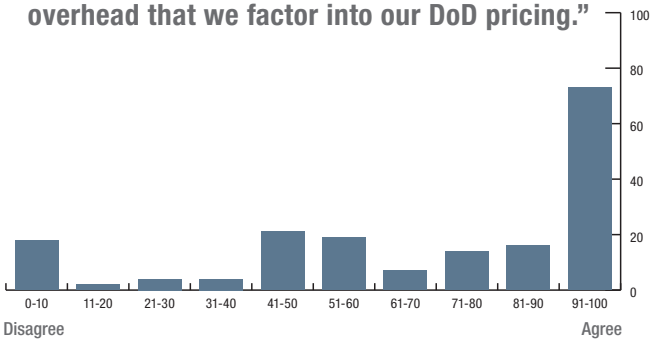
What security measures does your company use?



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



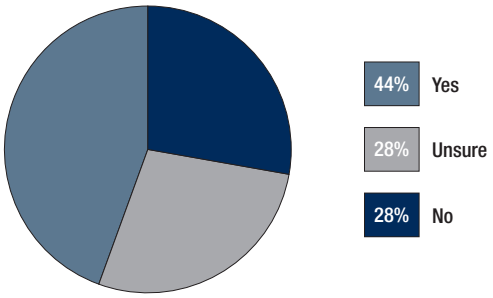
"We view DFARS 7012 costs as part of our corporate overhead that we factor into our DoD pricing."



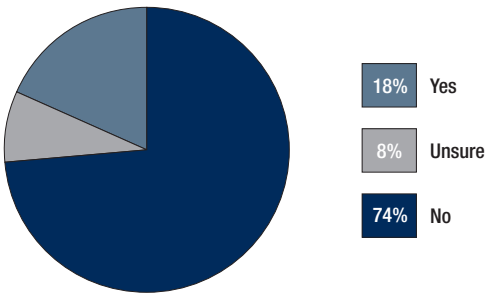
Survey participants were asked to rate their agreement with the statements above on a scale of 0-100.

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

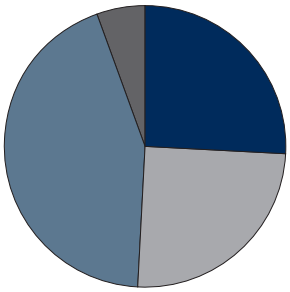
Other Than Small Business



Small Business

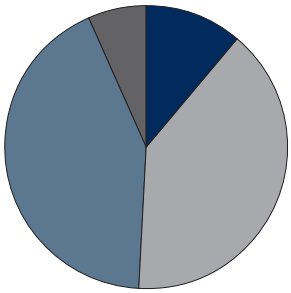


If you are a prime contractor, is (are) your subcontractor(s) in compliance with DFARS 7012 regulations?



- 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

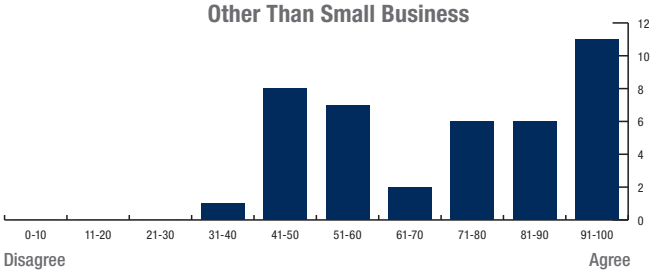
If you are a subcontractor, has (have) your prime contractor(s) provided you with information about how to comply with the DFARS 7012 regulations?



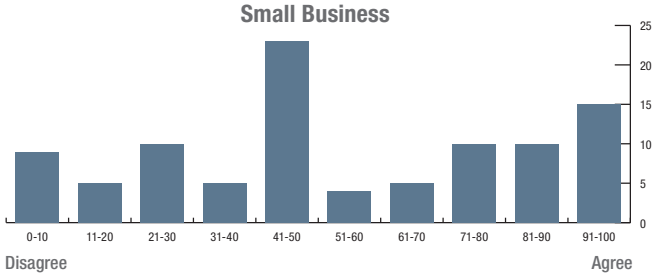
- 6% — Not at all – we do not handle controlled unclassified information (CUI)
- 43% — No – we saw it as a flow-down in our subcontract
- 40% — Yes – our prime(s) made us aware of the requirement
- 11% — Definitely – our prime(s) has (have) provided information on how to comply and has (have) accessible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

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

Other Than Small Business

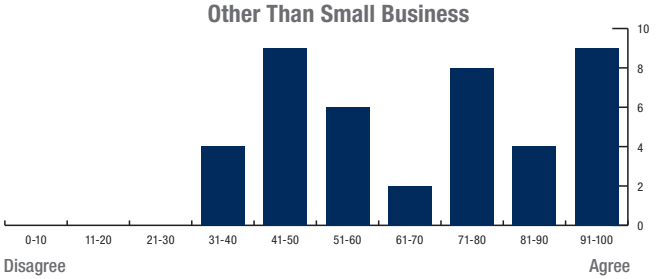


Small Business

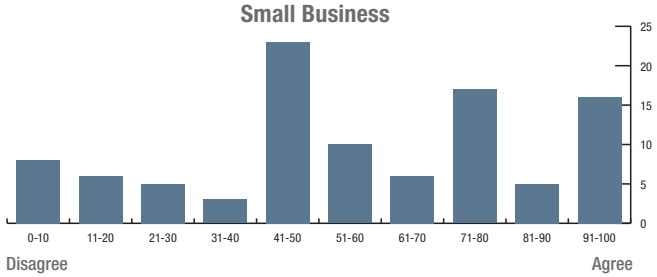


How confident are you in your ability to recover from a cyber incident in 24 hours?

Other Than Small Business

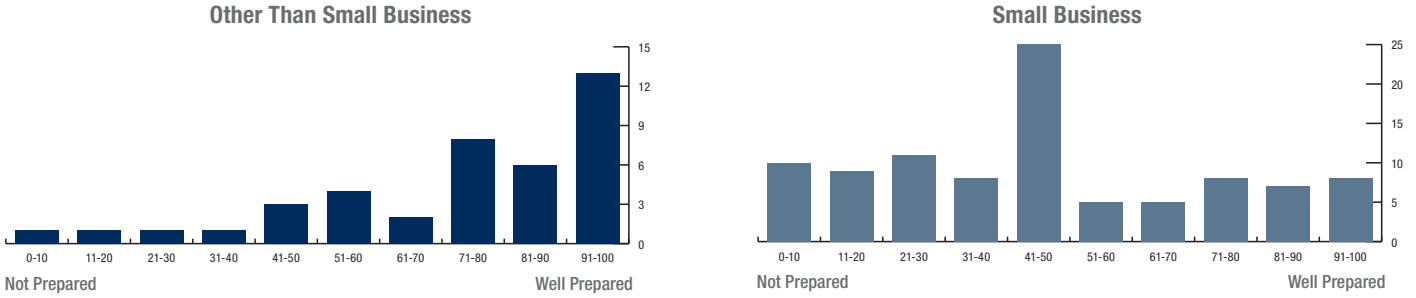


Small Business



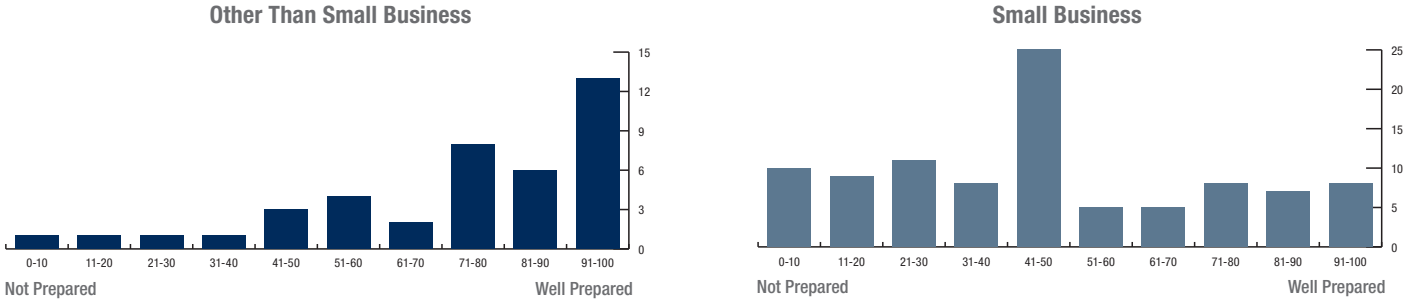
Survey participants were asked to rate their agreement with the statements above on a scale of 0-100.

How adequate do you think the DFARS 7012 and NIST SP 800-171 guidance is to achieve a comprehensive level of security?



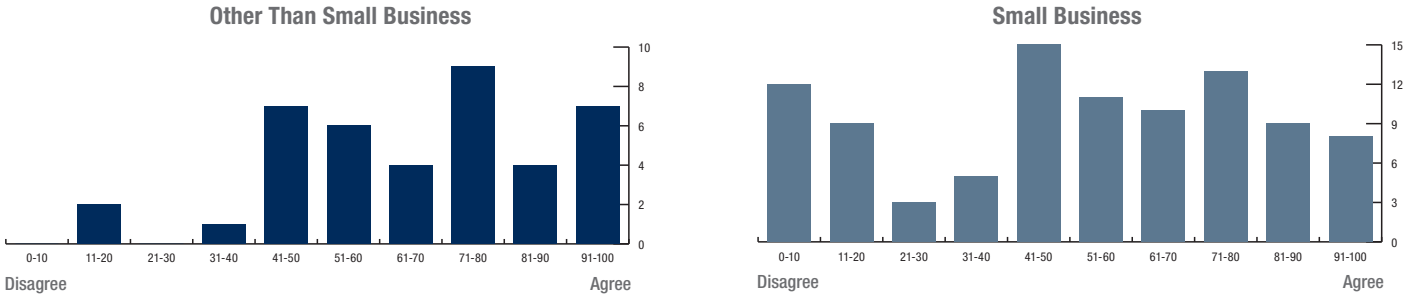
Survey participants were asked to rate their agreement with the statements above on a scale of 0-100.

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



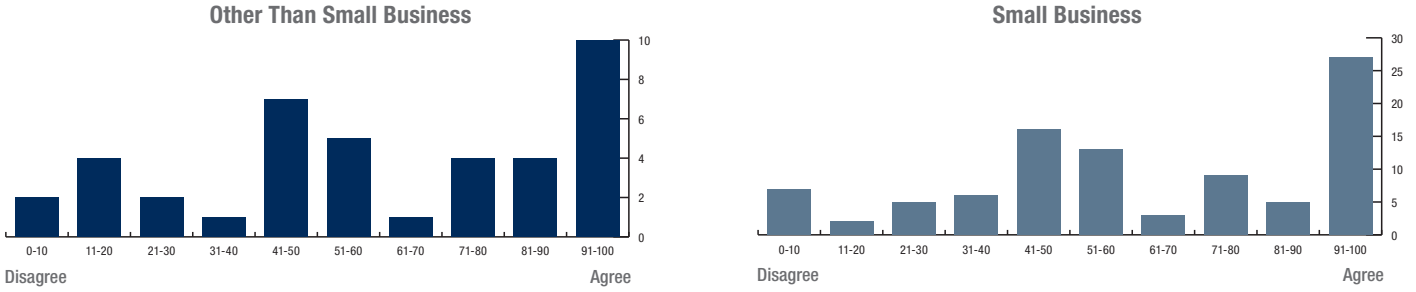
Survey participants were asked to rate their level of preparedness on a scale of 0-100.

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



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."



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.

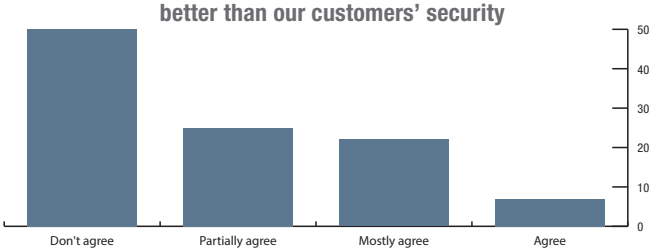
12% have attended DFARS 7012 requirements education or training at their local PTAC and/or NIST MEP Center.

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

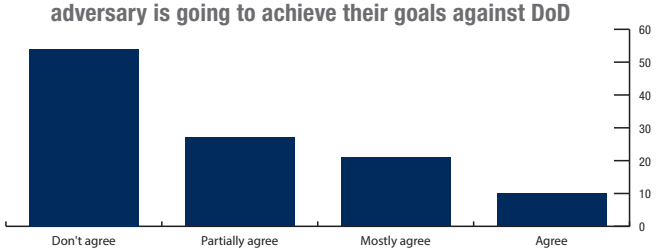
7% have attended DFARS 7012 requirements education or training from their prime contractor.

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

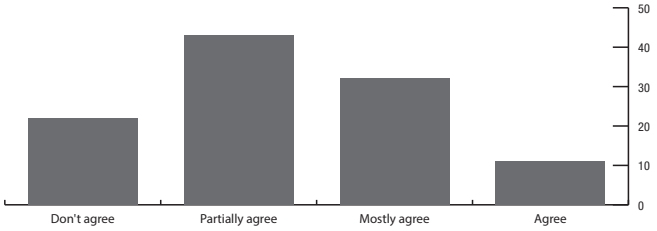
No improvement – my company's security is better than our customers' security



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

	Number of Employees	Percentage of Participants
Small Business	1 to 50	34%
	51 to 250	19.5%
	251 to 500	5%
Other than Small Business	501 to 1000	6%
	1001 to 2000	5%
	2001 +	30%

FOR MORE INFORMATION, CONTACT

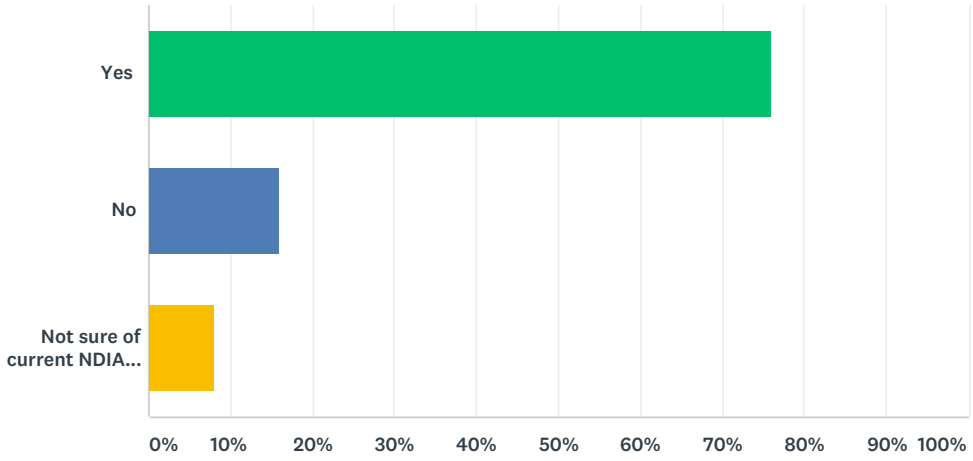
Regulatory@NDIA.org or visit NDIA.org/Divisions/Cybersecurity

APPENDIX B

DoD's NIST 800-171 and DFARS 252-204.7012 Impacts on Small Business:
Survey Results Micro Small Businesses

Q1 Are you an NDIA member?

Answered: 50 Skipped: 0



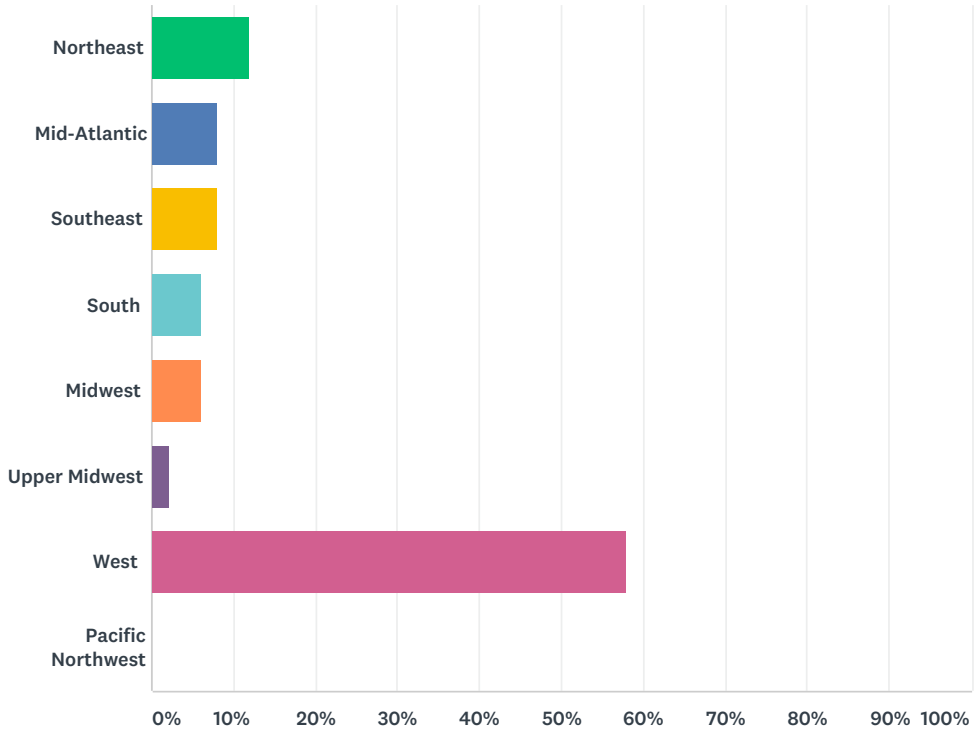
ANSWER CHOICES	RESPONSES	
Yes	76.00%	38
No	16.00%	8
Not sure of current NDIA membership status	8.00%	4
TOTAL		50

Q2 How long has your company been in existence?

Answered: 46 Skipped: 4

Q3 In what region of the country is your company headquartered?

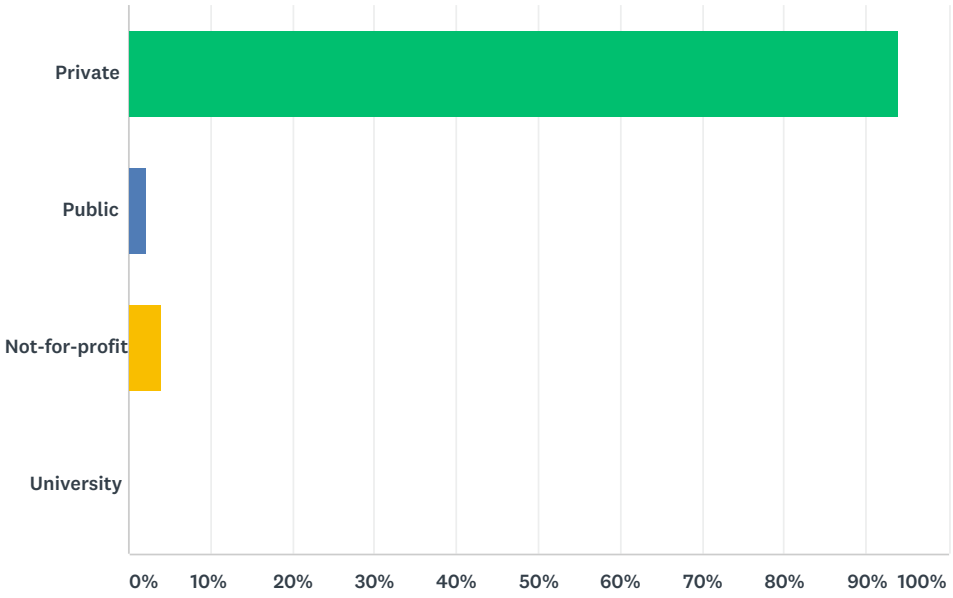
Answered: 50 Skipped: 0



ANSWER CHOICES	RESPONSES	
Northeast	12.00%	6
Mid-Atlantic	8.00%	4
Southeast	8.00%	4
South	6.00%	3
Midwest	6.00%	3
Upper Midwest	2.00%	1
West	58.00%	29
Pacific Northwest	0.00%	0
TOTAL		50

Q4 What type of entity is your company?

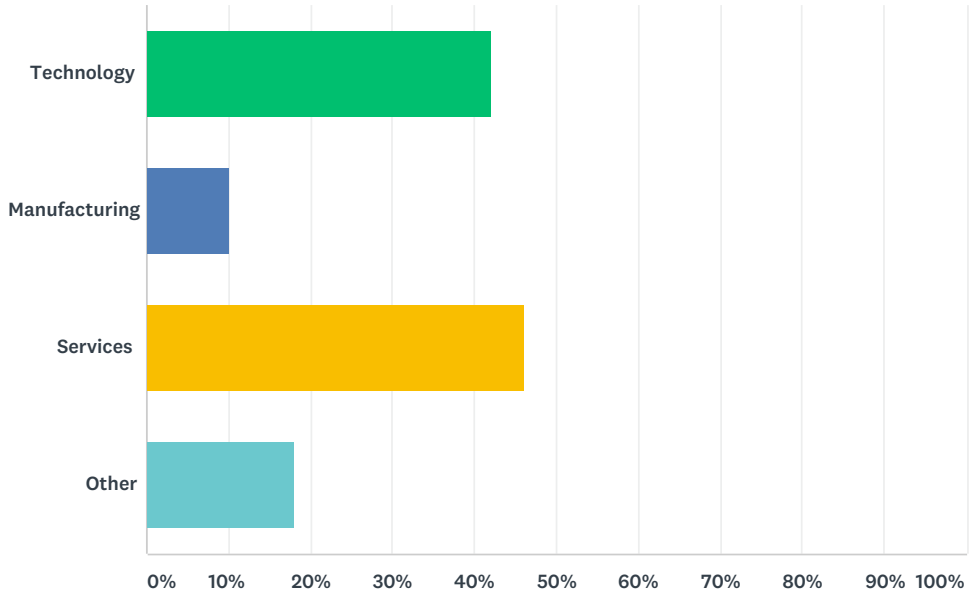
Answered: 50 Skipped: 0



ANSWER CHOICES	RESPONSES	
Private	94.00%	47
Public	2.00%	1
Not-for-profit	4.00%	2
University	0.00%	0
TOTAL		50

Q5 What industry is your government contracting work primarily in:

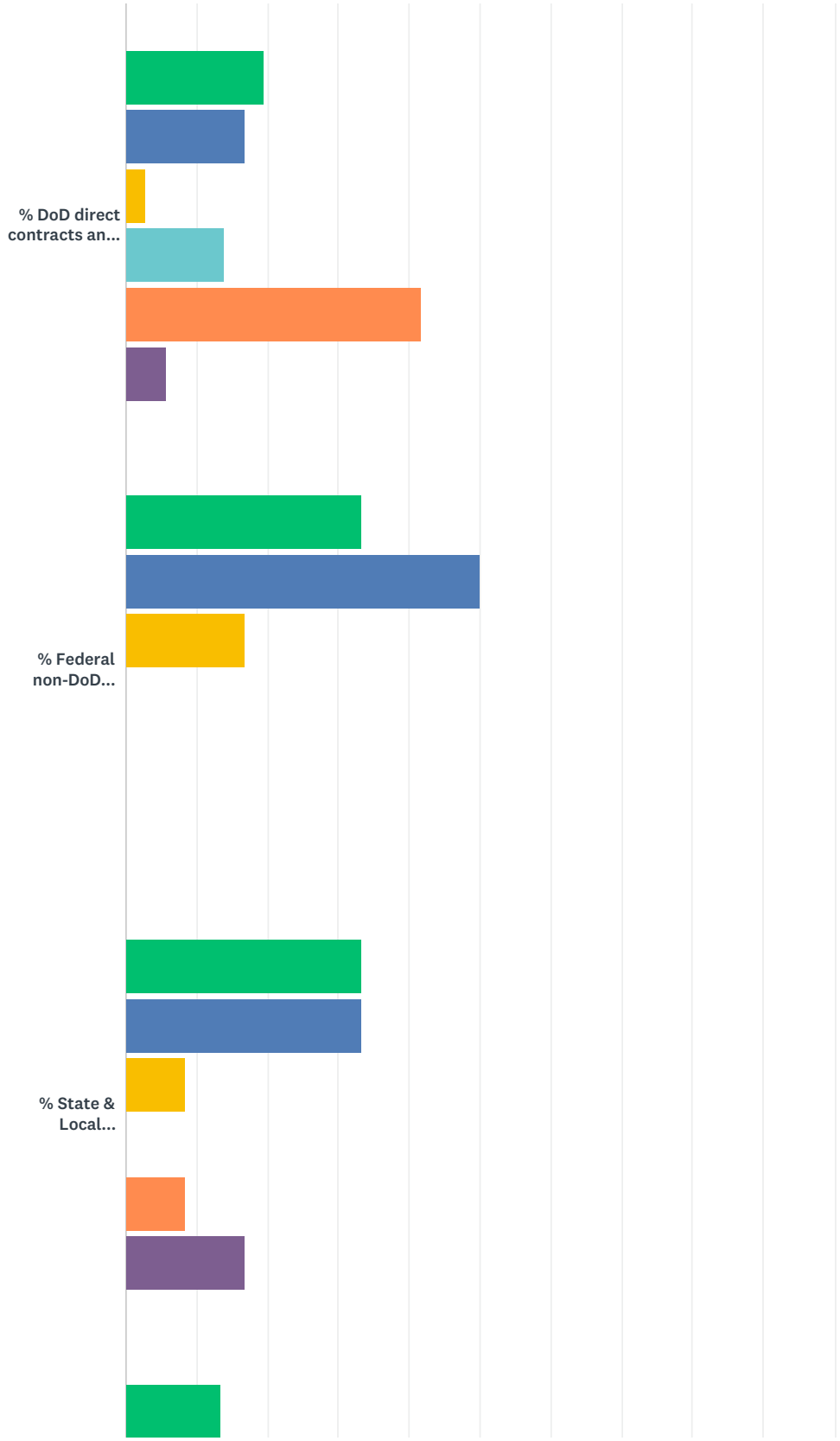
Answered: 50 Skipped: 0

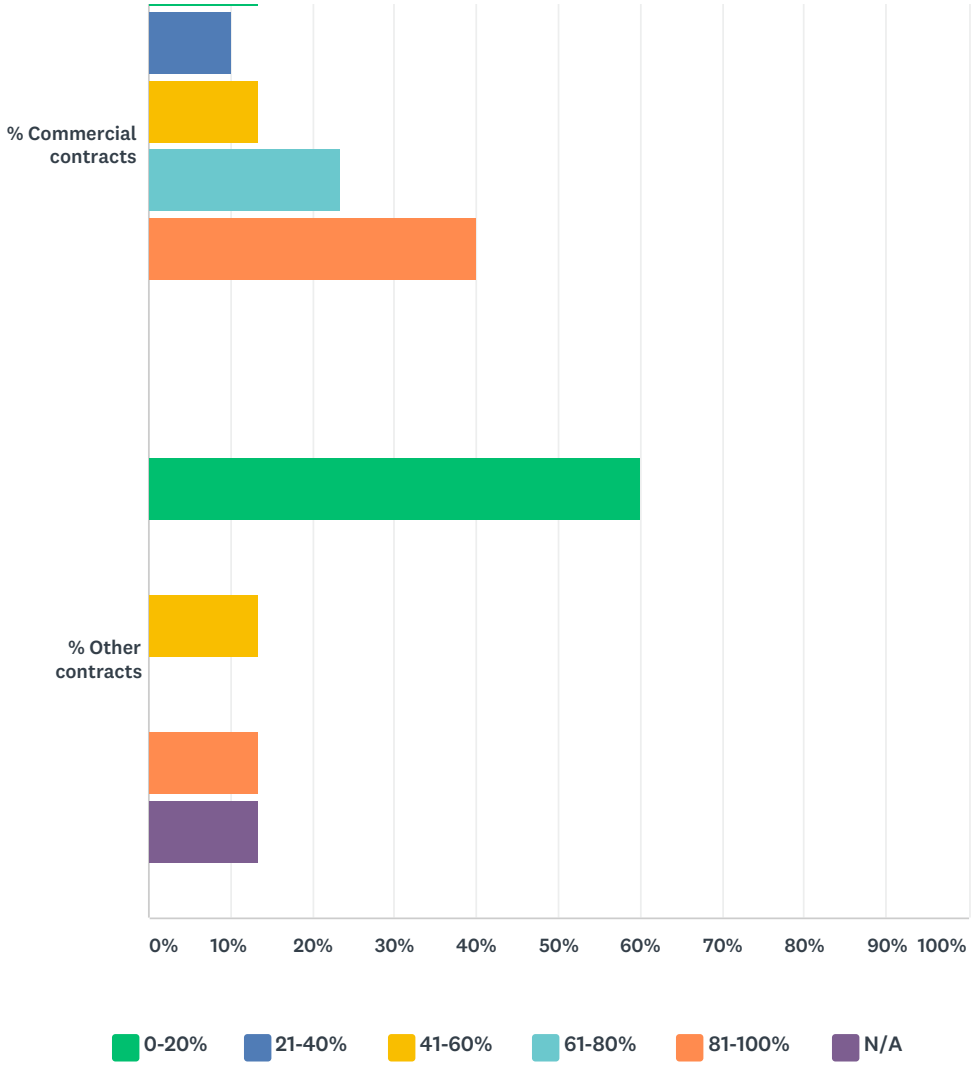


ANSWER CHOICES	RESPONSES	
Technology	42.00%	21
Manufacturing	10.00%	5
Services	46.00%	23
Other	18.00%	9
Total Respondents: 50		

Q6 Please provide percentages of business based on revenue, that total 100%

Answered: 49 Skipped: 1

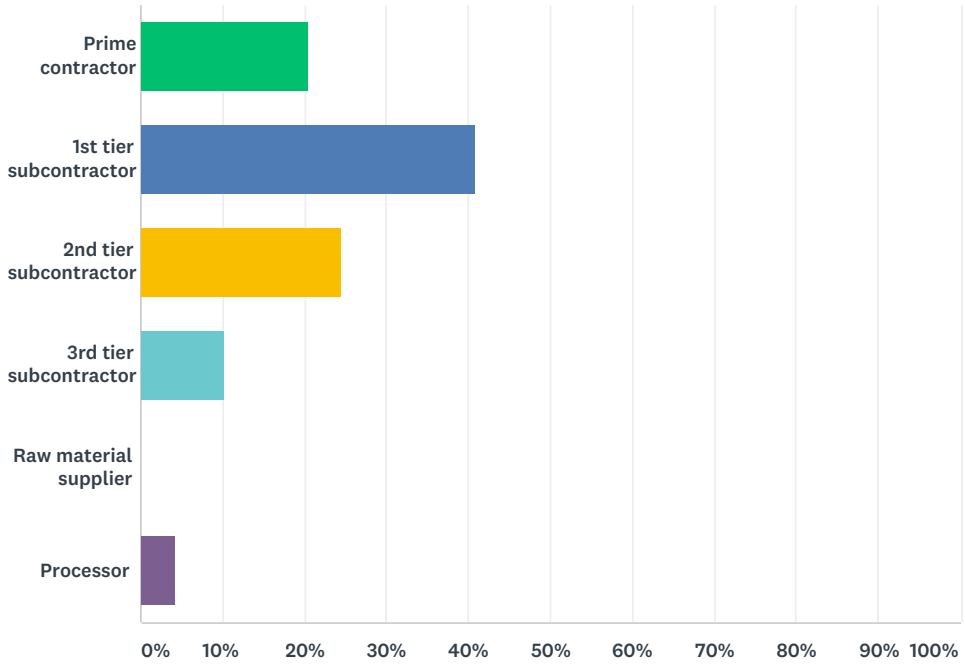




	0-20%	21-40%	41-60%	61-80%	81-100%	N/A	TOTAL	WEIGHTED AVERAGE
% DoD direct contracts and subcontracts	19.44% 7	16.67% 6	2.78% 1	13.89% 5	41.67% 15	5.56% 2	36	3.44
% Federal non-DoD contracts	33.33% 2	50.00% 3	16.67% 1	0.00% 0	0.00% 0	0.00% 0	6	1.83
% State & Local (including State/Local Education) government contracts	33.33% 4	33.33% 4	8.33% 1	0.00% 0	8.33% 1	16.67% 2	12	2.00
% Commercial contracts	13.33% 4	10.00% 3	13.33% 4	23.33% 7	40.00% 12	0.00% 0	30	3.67
% Other contracts	60.00% 9	0.00% 0	13.33% 2	0.00% 0	13.33% 2	13.33% 2	15	1.92

Q7 What is your company's primary position in the supply chain?

Answered: 49 Skipped: 1



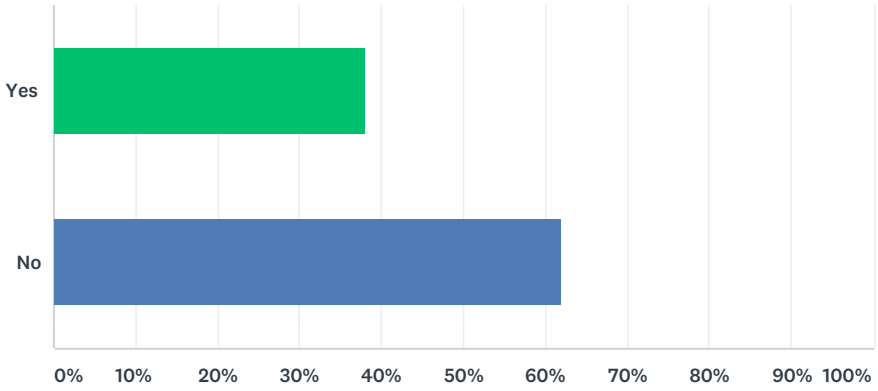
ANSWER CHOICES	RESPONSES	
Prime contractor	20.41%	10
1st tier subcontractor	40.82%	20
2nd tier subcontractor	24.49%	12
3rd tier subcontractor	10.20%	5
Raw material supplier	0.00%	0
Processor	4.08%	2
TOTAL		49

Q8 What is the number of employees in your company?

Answered: 50 Skipped: 0

Q9 Does your company perform classified work on behalf of the DoD?

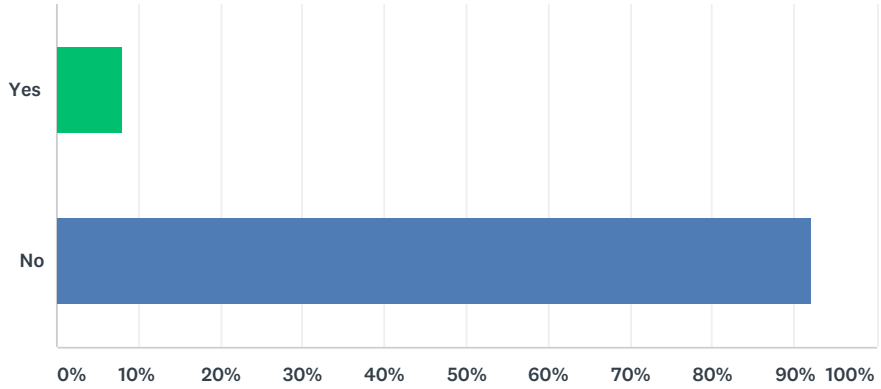
Answered: 50 Skipped: 0



ANSWER CHOICES	RESPONSES	
Yes	38.00%	19
No	62.00%	31
TOTAL		50

Q10 Does your company support power, water, alarm, environmental, or other utility equipment or services for the DoD?

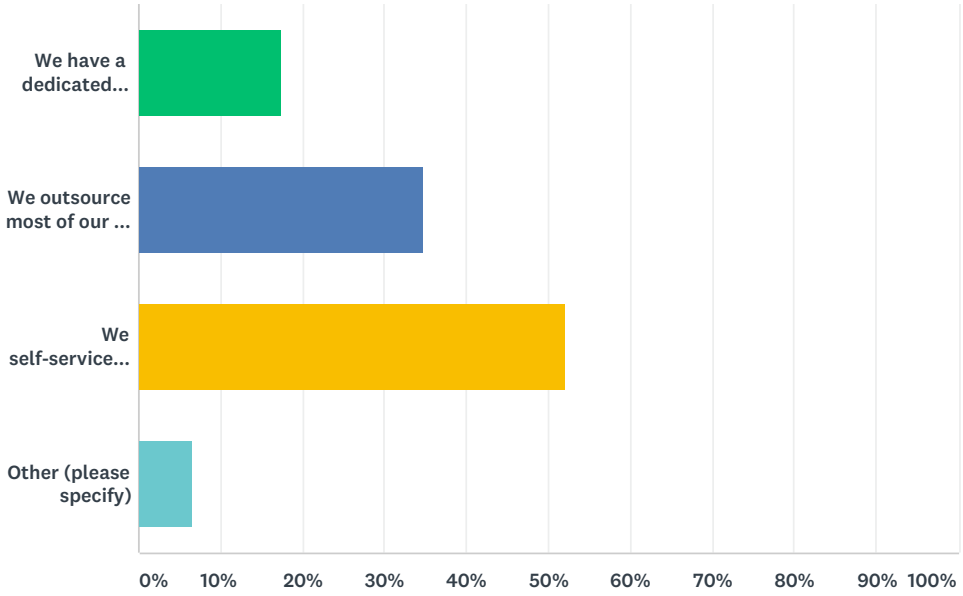
Answered: 50 Skipped: 0



ANSWER CHOICES	RESPONSES	
Yes	8.00%	4
No	92.00%	46
TOTAL		50

Q11 What type of IT services does your company use? (Select all that apply)

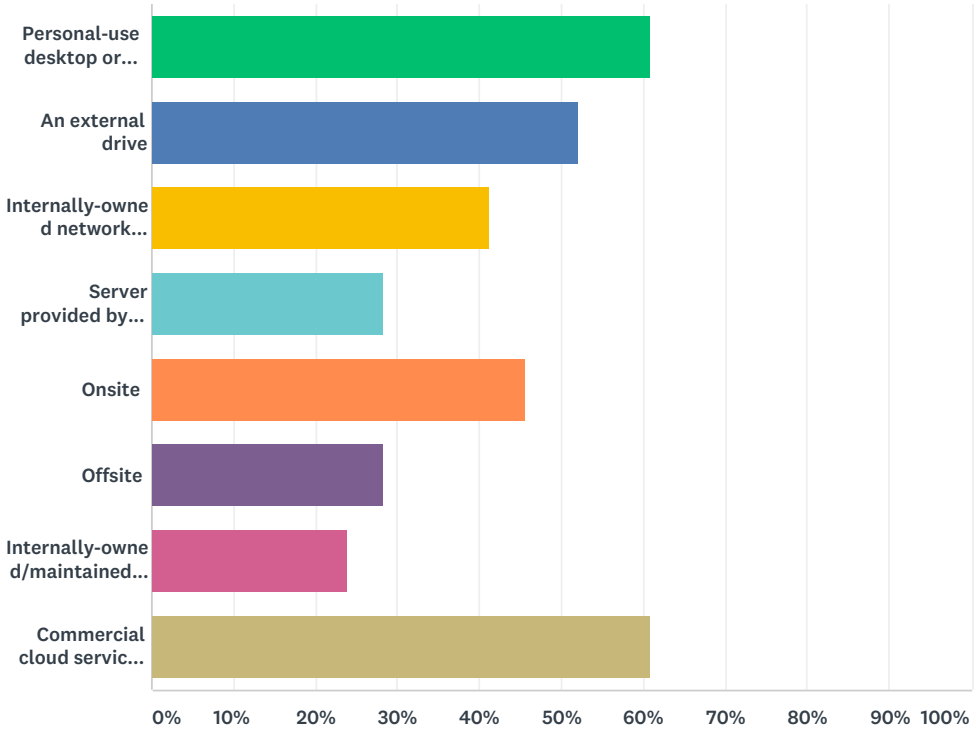
Answered: 46 Skipped: 4



ANSWER CHOICES	RESPONSES	
We have a dedicated in-house IT person or department	17.39%	8
We outsource most of our IT support to an external provider	34.78%	16
We self-service but do not have staff dedicated	52.17%	24
Other (please specify)	6.52%	3
Total Respondents: 46		

Q12 At your company, which of the following are possible methods to store data and documents? Select all that apply

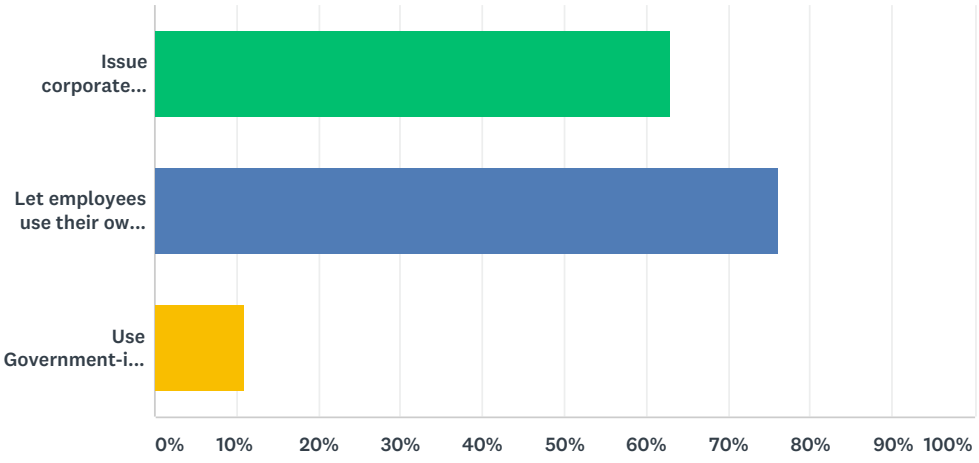
Answered: 46 Skipped: 4



ANSWER CHOICES	RESPONSES	
Personal-use desktop or laptop only	60.87%	28
An external drive	52.17%	24
Internally-owned network storage	41.30%	19
Server provided by managed-services company	28.26%	13
Onsite	45.65%	21
Offsite	28.26%	13
Internally-owned/maintained (private) cloud server	23.91%	11
Commercial cloud service (for example, Microsoft OneDrive, Apple iCloud, or Amazon Web Services)	60.87%	28
Total Respondents: 46		

Q13 Does your company (Select all that apply)

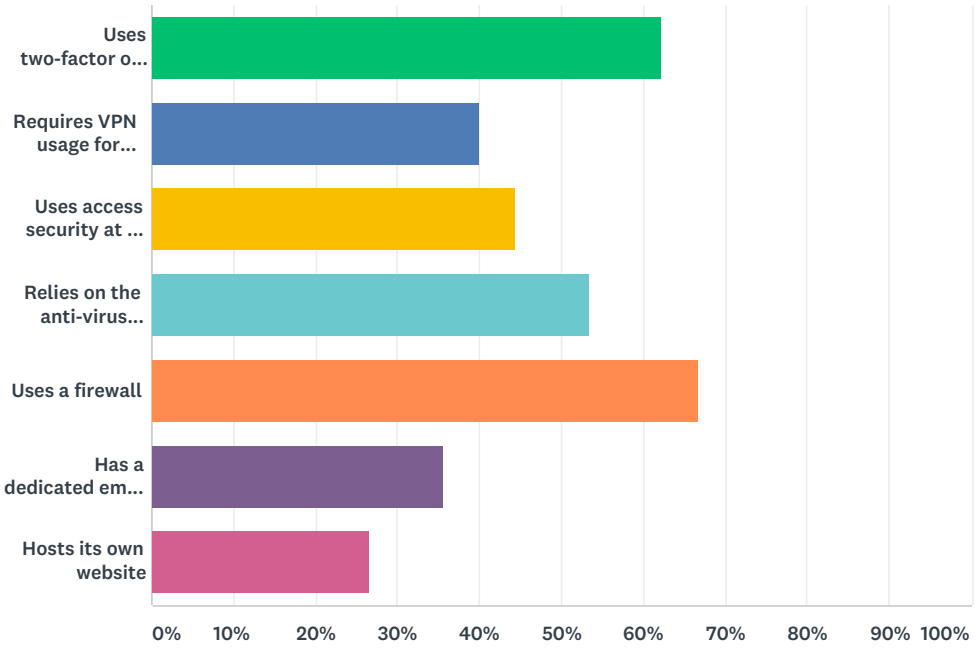
Answered: 46 Skipped: 4



ANSWER CHOICES	RESPONSES	
Issue corporate mobile phones, laptops or tablets for mobile use	63.04%	29
Let employees use their own mobile phones, laptops or tablets for corporate purposes	76.09%	35
Use Government-issued devices	10.87%	5
Total Respondents: 46		

Q14 Currently, my company (Select all that apply)

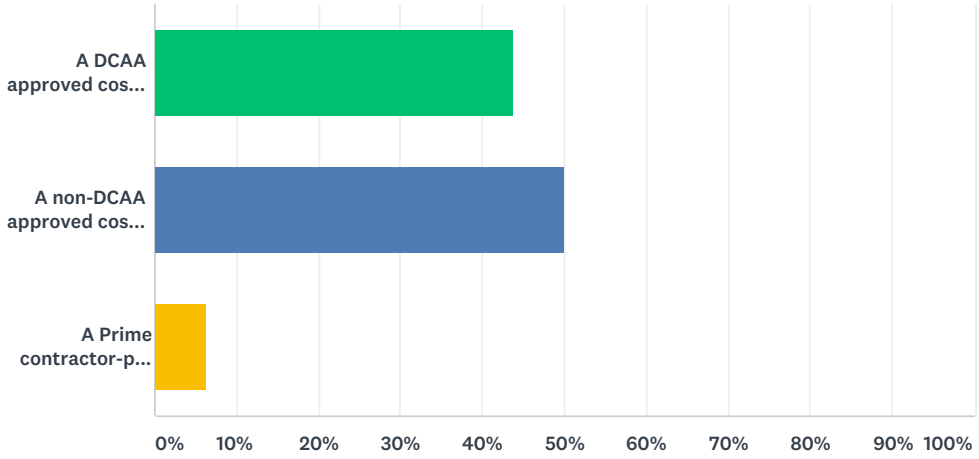
Answered: 45 Skipped: 5



ANSWER CHOICES	RESPONSES	
Uses two-factor or multi-factor authentication for log-ons	62.22%	28
Requires VPN usage for remote work	40.00%	18
Uses access security at the workspace in addition to door locks	44.44%	20
Relies on the anti-virus software that came installed on our equipment	53.33%	24
Uses a firewall	66.67%	30
Has a dedicated email server	35.56%	16
Hosts its own website	26.67%	12
Total Respondents: 45		

Q15 Does your company use any of the following accounting systems? (Select all that apply)

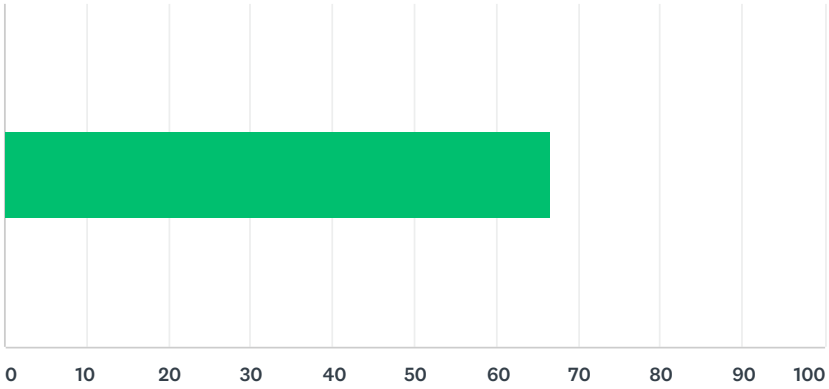
Answered: 32 Skipped: 18



ANSWER CHOICES	RESPONSES	
A DCAA approved cost accounting system	43.75%	14
A non-DCAA approved cost accounting system	50.00%	16
A Prime contractor-provided cost accounting system	6.25%	2
Total Respondents: 32		

Q16 How much do you agree with this statement? “We view security costs as being part of our corporate overhead that we factor into our DoD pricing.”

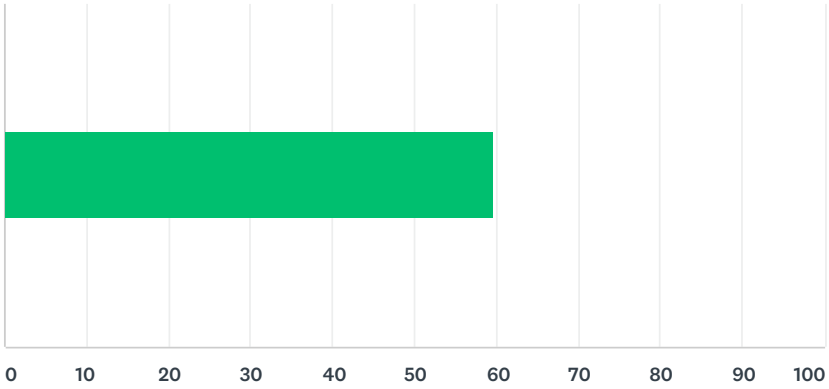
Answered: 40 Skipped: 10



ANSWER CHOICES	AVERAGE NUMBER	TOTAL NUMBER	RESPONSES
	67	2,662	40
Total Respondents: 40			

Q17 How much do you agree with this statement? “We view DFARS 7012 costs as being part of our corporate overhead that we factor into our DoD pricing.”

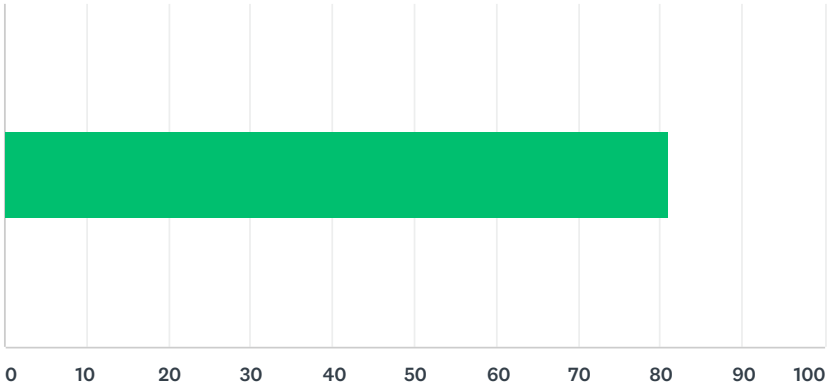
Answered: 40 Skipped: 10



ANSWER CHOICES	AVERAGE NUMBER	TOTAL NUMBER	RESPONSES
	60	2,387	40
Total Respondents: 40			

Q18 How much do you agree with this statement? “We should be able to directly charge DoD for the costs of complying with its specific DFARS 7012 requirements.”

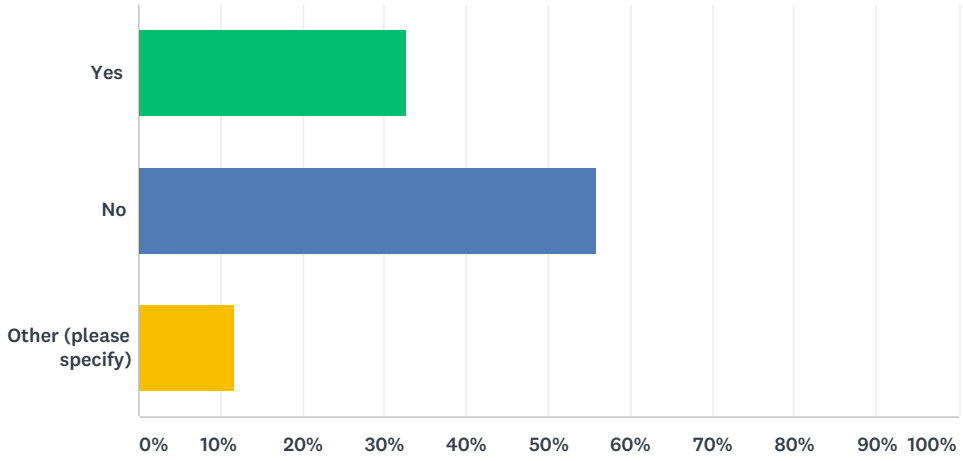
Answered: 41 Skipped: 9



ANSWER CHOICES	AVERAGE NUMBER	TOTAL NUMBER	RESPONSES
	81	3,320	41
Total Respondents: 41			

Q19 If you are still meeting the initial requirements of DFARS 7012 (e.g., developing or implementing your Plan of Actions and Milestones), have you estimated the costs of becoming compliant with DFARS 7012 requirements?

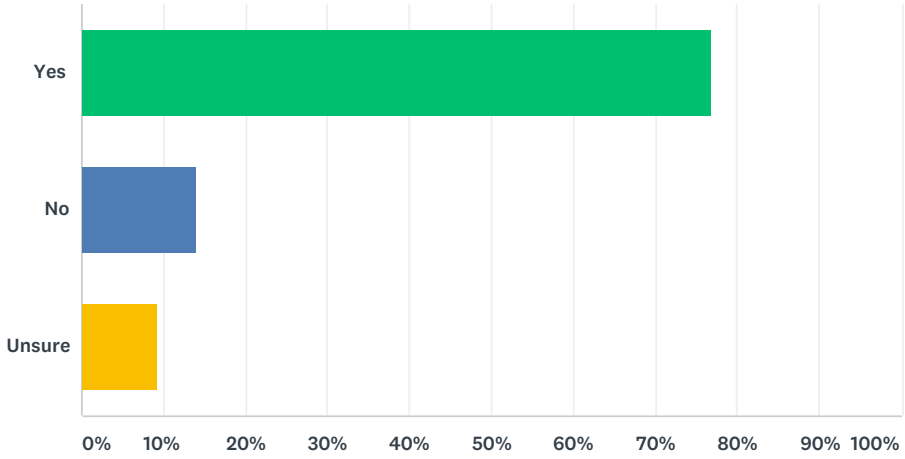
Answered: 43 Skipped: 7



ANSWER CHOICES	RESPONSES	
Yes	32.56%	14
No	55.81%	24
Other (please specify)	11.63%	5
TOTAL		43

Q20 Does your company estimate that ongoing compliance with DFARS 7012 is going to be a cost driver?

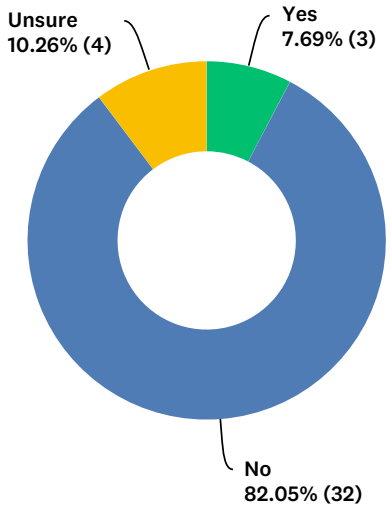
Answered: 43 Skipped: 7



ANSWER CHOICES	RESPONSES	
Yes	76.74%	33
No	13.95%	6
Unsure	9.30%	4
TOTAL		43

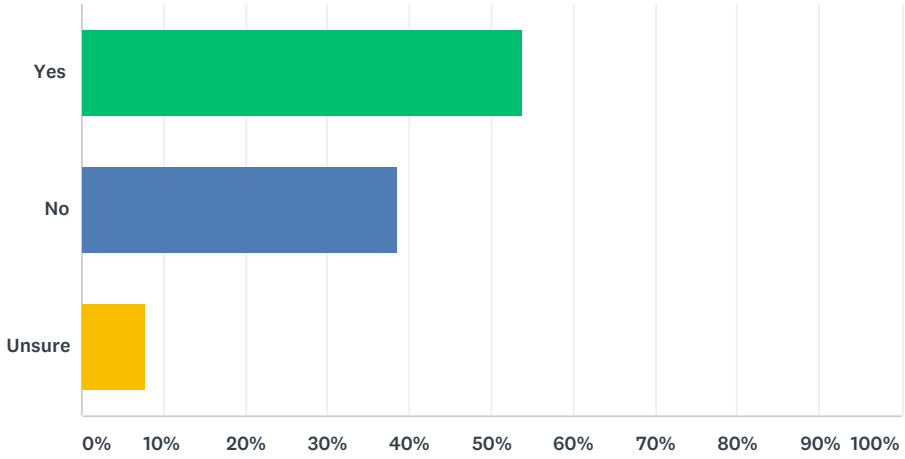
Q21 Has your company ever been the victim of a successful cyber attack?

Answered: 39 Skipped: 11



Q22 Does your company have a sense of the cost for responding to / recovering from a cybersecurity incident?

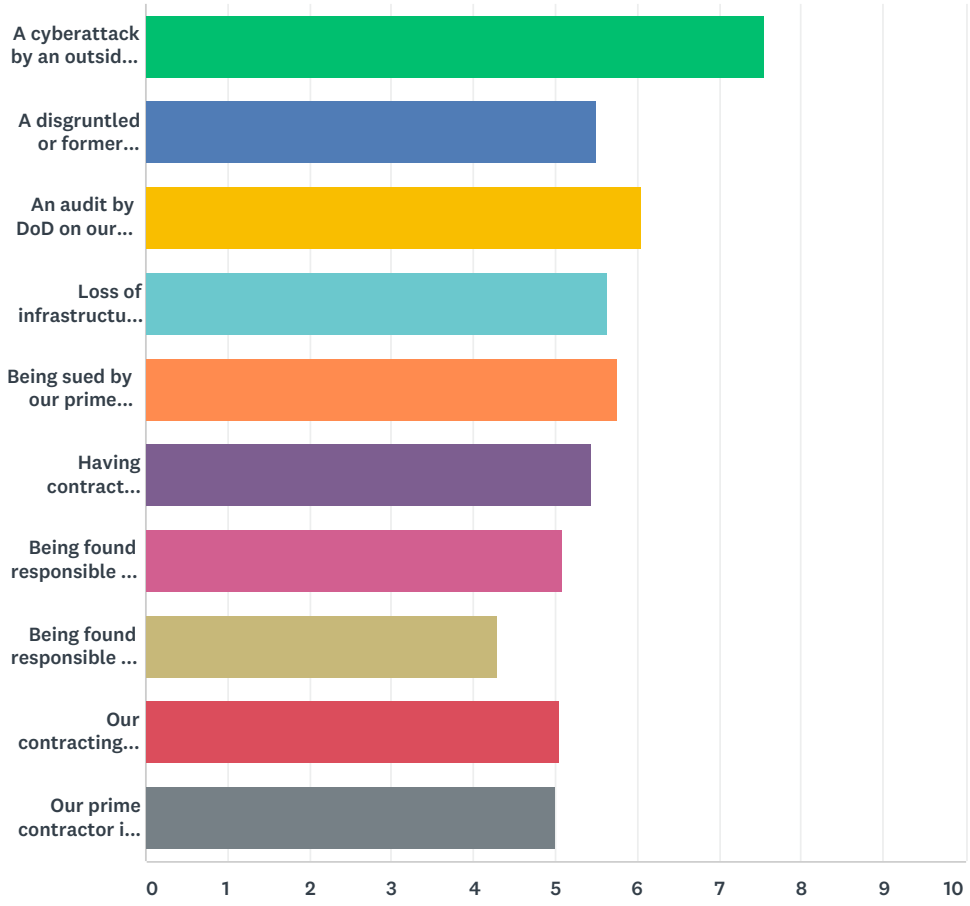
Answered: 39 Skipped: 11



ANSWER CHOICES	RESPONSES	
Yes	53.85%	21
No	38.46%	15
Unsure	7.69%	3
TOTAL		39

Q23 In your perception, which of these is the biggest threat? Please rank these in order of importance to your company, with 1 being most important and 10 being least important.

Answered: 39 Skipped: 11

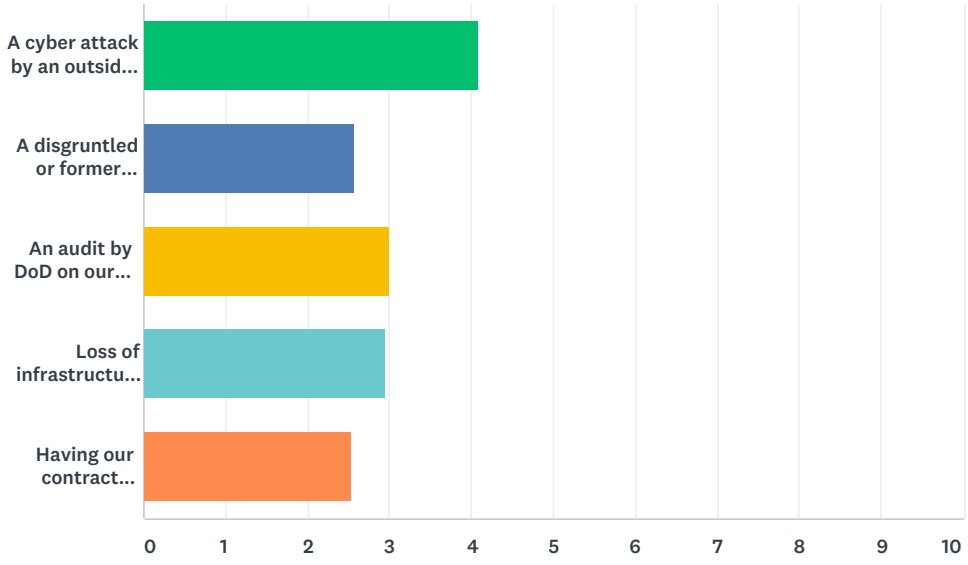


	1	2	3	4	5	6	7	8	9	10	TOTAL	SCOR
A cyberattack by an outside actor	44.74% 17	2.63% 1	10.53% 4	7.89% 3	7.89% 3	10.53% 4	5.26% 2	5.26% 2	2.63% 1	2.63% 1	38	7.
A disgruntled or former employee wreaking havoc on our systems	11.43% 4	17.14% 6	8.57% 3	5.71% 2	8.57% 3	11.43% 4	2.86% 1	5.71% 2	8.57% 3	20.00% 7	35	5.
An audit by DoD on our cybersecurity program	2.70% 1	18.92% 7	13.51% 5	10.81% 4	21.62% 8	5.41% 2	10.81% 4	0.00% 0	8.11% 3	8.11% 3	37	6.

Loss of infrastructure (for example, power outage, fire, or environmental event) that could degrade our cybersecurity	10.81% 4	16.22% 6	5.41% 2	16.22% 6	0.00% 0	8.11% 3	8.11% 3	16.22% 6	10.81% 4	8.11% 3	37	5.
Being sued by our prime contractor for noncompliance	0.00% 0	8.33% 3	11.11% 4	19.44% 7	19.44% 7	16.67% 6	5.56% 2	13.89% 5	5.56% 2	0.00% 0	36	5.
Having contract recovery action taken against us by DoD or a prime for noncompliance	2.70% 1	8.11% 3	2.70% 1	16.22% 6	16.22% 6	18.92% 7	18.92% 7	8.11% 3	8.11% 3	0.00% 0	37	5.
Being found responsible for a major security breach that impacts personnel	2.70% 1	13.51% 5	10.81% 4	8.11% 3	5.41% 2	13.51% 5	2.70% 1	21.62% 8	18.92% 7	2.70% 1	37	5.
Being found responsible for a major security breach that impacts public safety	5.56% 2	5.56% 2	11.11% 4	2.78% 1	8.33% 3	2.78% 1	19.44% 7	5.56% 2	16.67% 6	22.22% 8	36	4.
Our contracting officer doesn't understand cybersecurity at all, and will impose unrealistic audit requirements	5.13% 2	7.69% 3	20.51% 8	2.56% 1	10.26% 4	5.13% 2	12.82% 5	7.69% 3	12.82% 5	15.38% 6	39	5.
Our prime contractor is going to use these requirements to squeeze us right off the contract	12.82% 5	5.13% 2	7.69% 3	12.82% 5	2.56% 1	7.69% 3	12.82% 5	12.82% 5	5.13% 2	20.51% 8	39	5.

Q24 How likely do you think each of these scenarios is? Please rank them in order of 1 (most likely) to 5 (least likely)

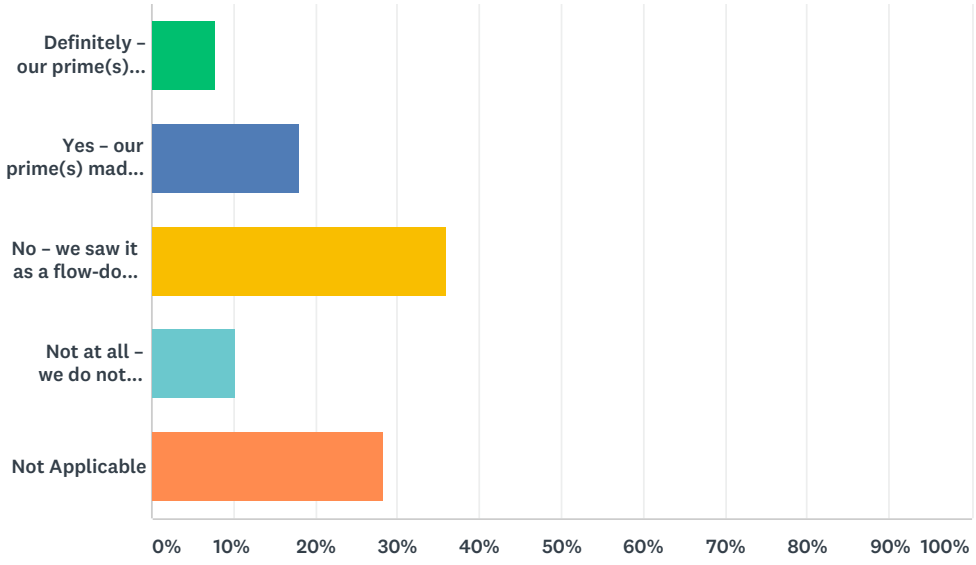
Answered: 39 Skipped: 11



	1	2	3	4	5	TOTAL	SCORE
A cyber attack by an outside actor	56.76% 21	18.92% 7	8.11% 3	8.11% 3	8.11% 3	37	4.08
A disgruntled or former employee wreaking havoc on our systems	6.06% 2	12.12% 4	39.39% 13	18.18% 6	24.24% 8	33	2.58
An audit by DoD on our cybersecurity program	8.33% 3	33.33% 12	19.44% 7	27.78% 10	11.11% 4	36	3.00
Loss of infrastructure (for example, power outage, fire, or environmental event) that could degrade our cybersecurity	21.62% 8	16.22% 6	16.22% 6	27.03% 10	18.92% 7	37	2.95
Having our contract rescinded by a contracting officer or a prime contractor because of poor cybersecurity implementation	7.89% 3	21.05% 8	21.05% 8	15.79% 6	34.21% 13	38	2.53

Q25 If you are a subcontractor, has your prime contractor(s) provided you with information about how to comply with the DFARS 7012 regulations?

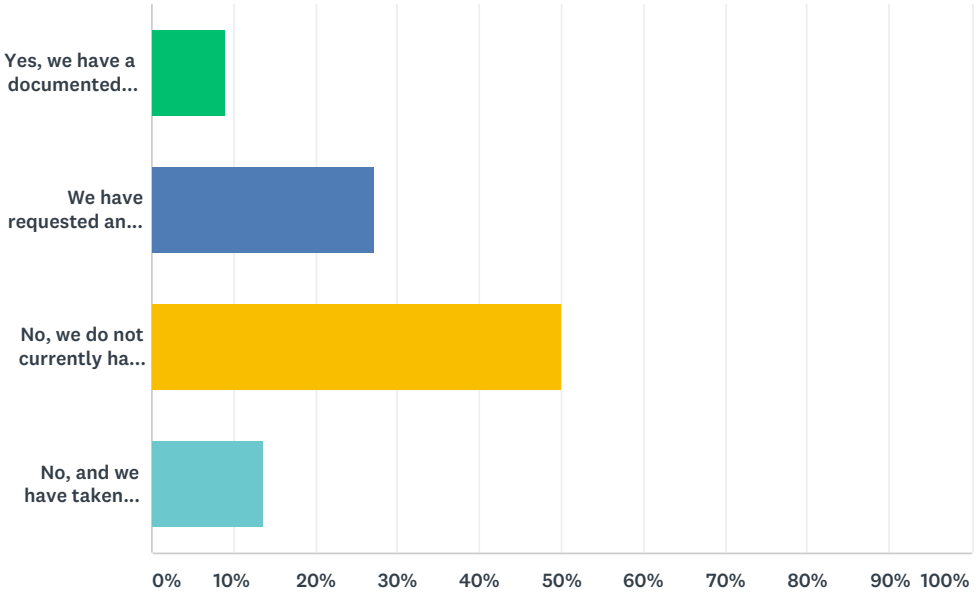
Answered: 39 Skipped: 11



ANSWER CHOICES	RESPONSES	
Definitely – our prime(s) has provided information on how to comply, and been accessible for questions and discussion	7.69%	3
Yes – our prime(s) made us aware of the requirement	17.95%	7
No – we saw it as a flow-down in our subcontract	35.90%	14
Not at all – we do not handle CUI	10.26%	4
Not Applicable	28.21%	11
TOTAL		39

Q26 If you are a Prime contractor, is (are) your subcontractor(s) in compliance with DFARS 7012 regulations?

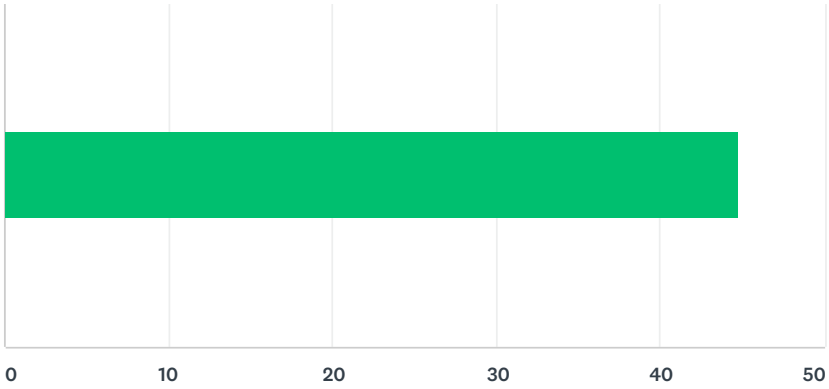
Answered: 22 Skipped: 28



ANSWER CHOICES	RESPONSES	
Yes, we have a documented System Security Plan (SSP) from the subcontractor	9.09%	2
We have requested an SSP from the subcontractor	27.27%	6
No, we do not currently have a documented SSP from the subcontractor	50.00%	11
No, and we have taken corrective action against the subcontractor	13.64%	3
TOTAL		22

Q27 How prepared, do you believe, is your company to comply with the DFARS 7012 requirements?

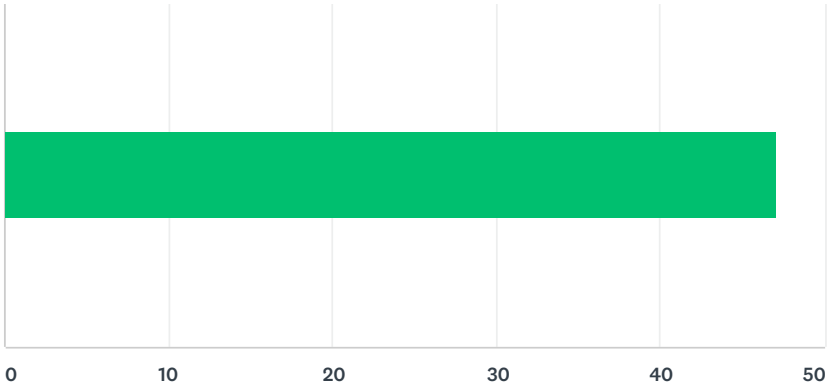
Answered: 37 Skipped: 13



ANSWER CHOICES	AVERAGE NUMBER	TOTAL NUMBER	RESPONSES
	45	1,658	37
Total Respondents: 37			

Q28 How confident are you in your ability to recover from a cyber incident in 24 hours?

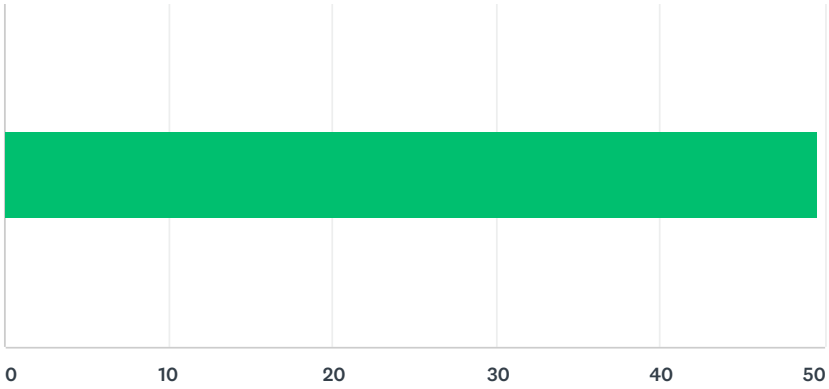
Answered: 39 Skipped: 11



ANSWER CHOICES	AVERAGE NUMBER	TOTAL NUMBER	RESPONSES
	47	1,837	39
Total Respondents: 39			

Q29 How adequate do you think the DFARS 7012 and NIST SP 800-171 guidance is, to achieve a comprehensive level of security?

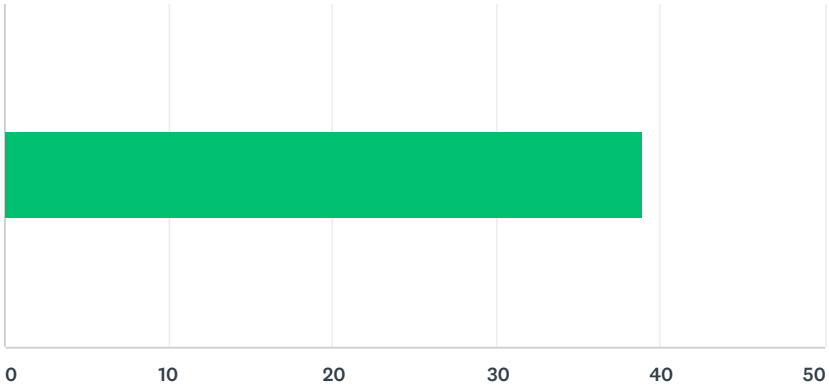
Answered: 37 Skipped: 13



ANSWER CHOICES	AVERAGE NUMBER	TOTAL NUMBER	RESPONSES
	50	1,835	37
Total Respondents: 37			

Q30 Rate your level of preparedness for a Defense Contract Managment Agency (DCMA) cybersecurity audit?

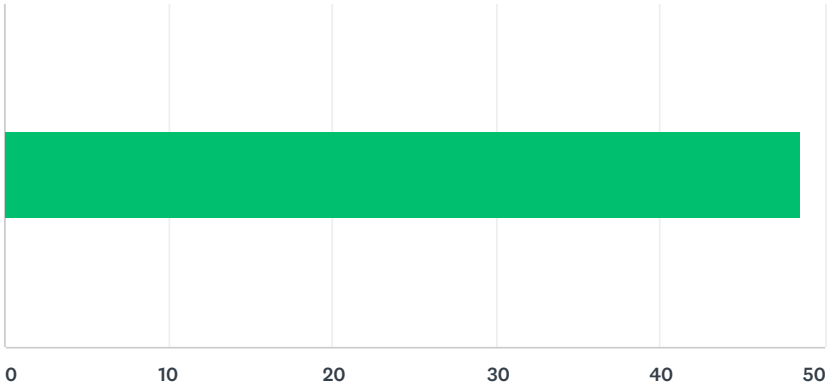
Answered: 37 Skipped: 13



ANSWER CHOICES	AVERAGE NUMBER	TOTAL NUMBER	RESPONSES
	39	1,439	37
Total Respondents: 37			

Q31 How much do you agree with this statement? "Our employees are well prepared to understand and respond to cybersecurity threats."

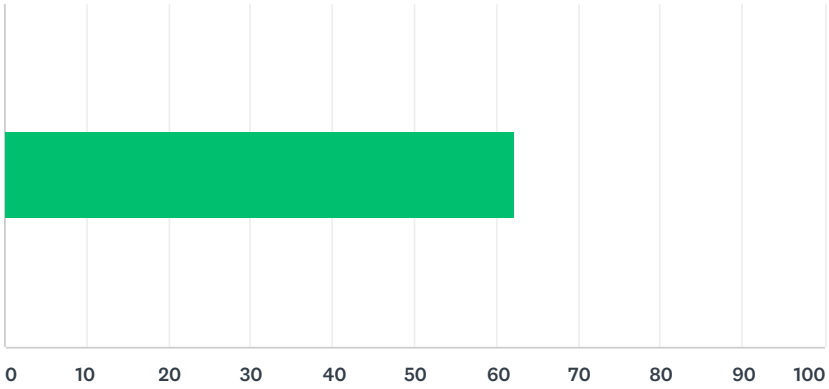
Answered: 37 Skipped: 13



ANSWER CHOICES	AVERAGE NUMBER	TOTAL NUMBER	RESPONSES
	49	1,797	37
Total Respondents: 37			

Q32 How much do you agree with this statement? "Our senior management has communicated that 7012 compliance is a priority."

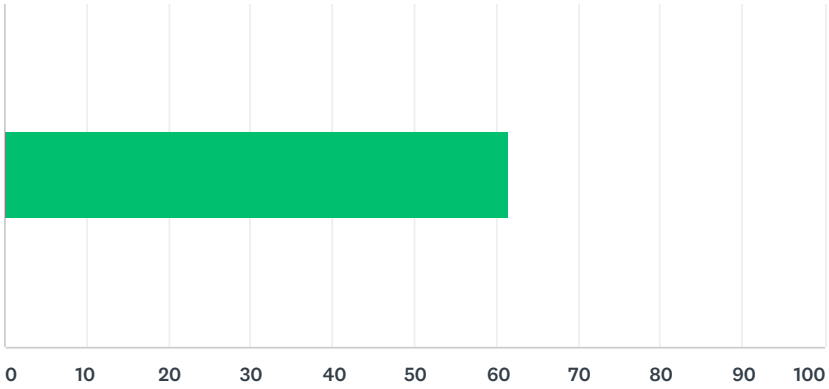
Answered: 35 Skipped: 15



ANSWER CHOICES	AVERAGE NUMBER	TOTAL NUMBER	RESPONSES
	62	2,174	35
Total Respondents: 35			

Q33 How much do you agree with this statement? "We may need outside consulting to help us comply with DFARS 7012 requirements."

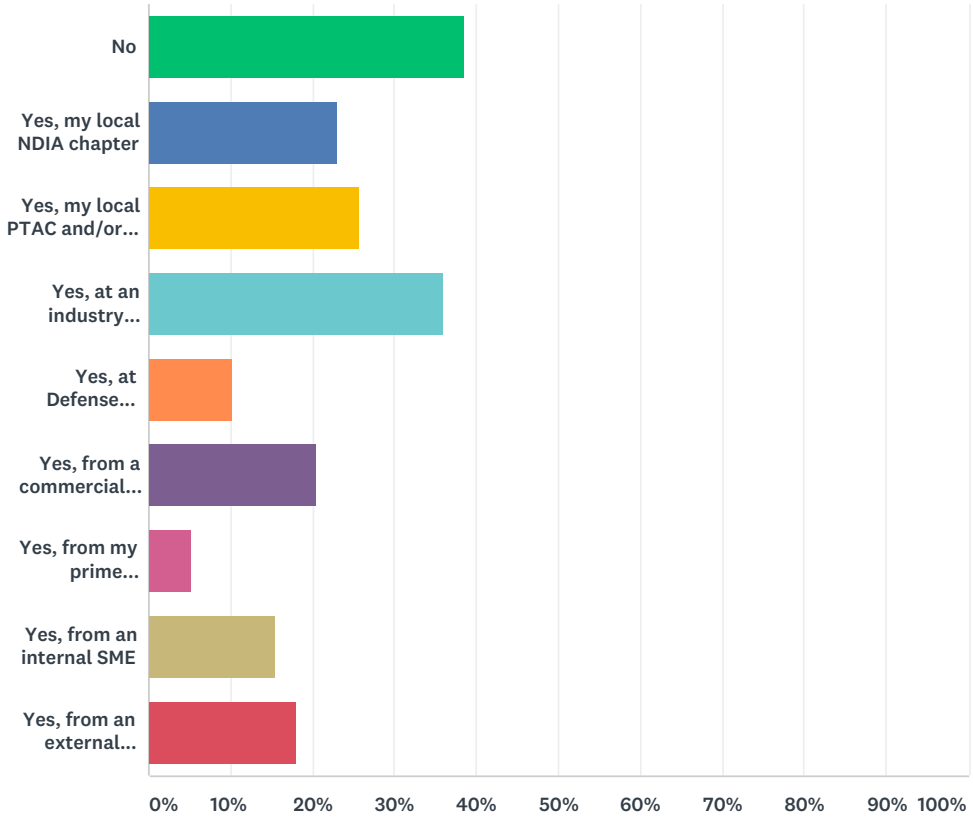
Answered: 37 Skipped: 13



ANSWER CHOICES	AVERAGE NUMBER	TOTAL NUMBER	RESPONSES
	61	2,273	37
Total Respondents: 37			

Q34 Have you attended any outside education or training for DFARS 7012 requirements? [select all that apply]

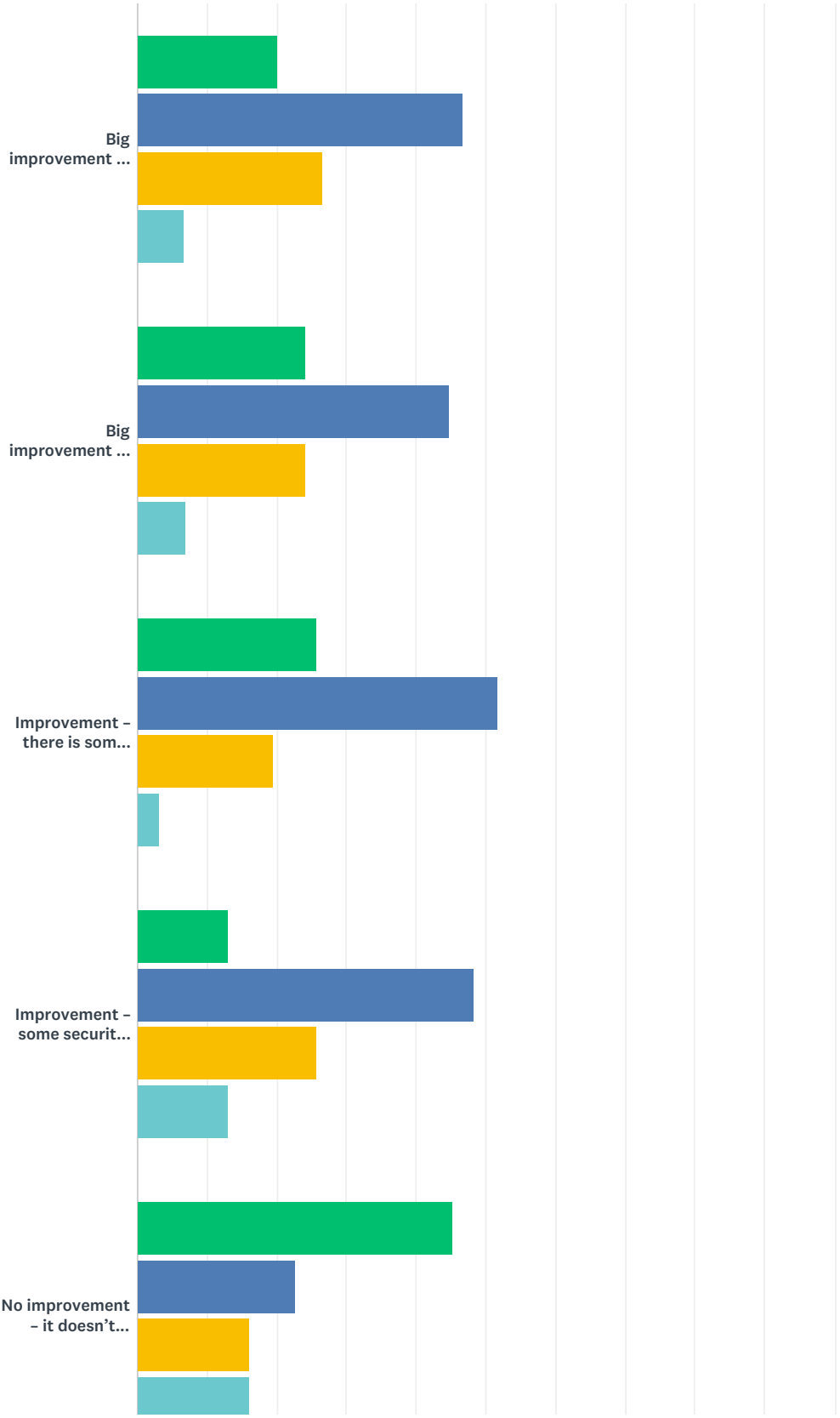
Answered: 39 Skipped: 11

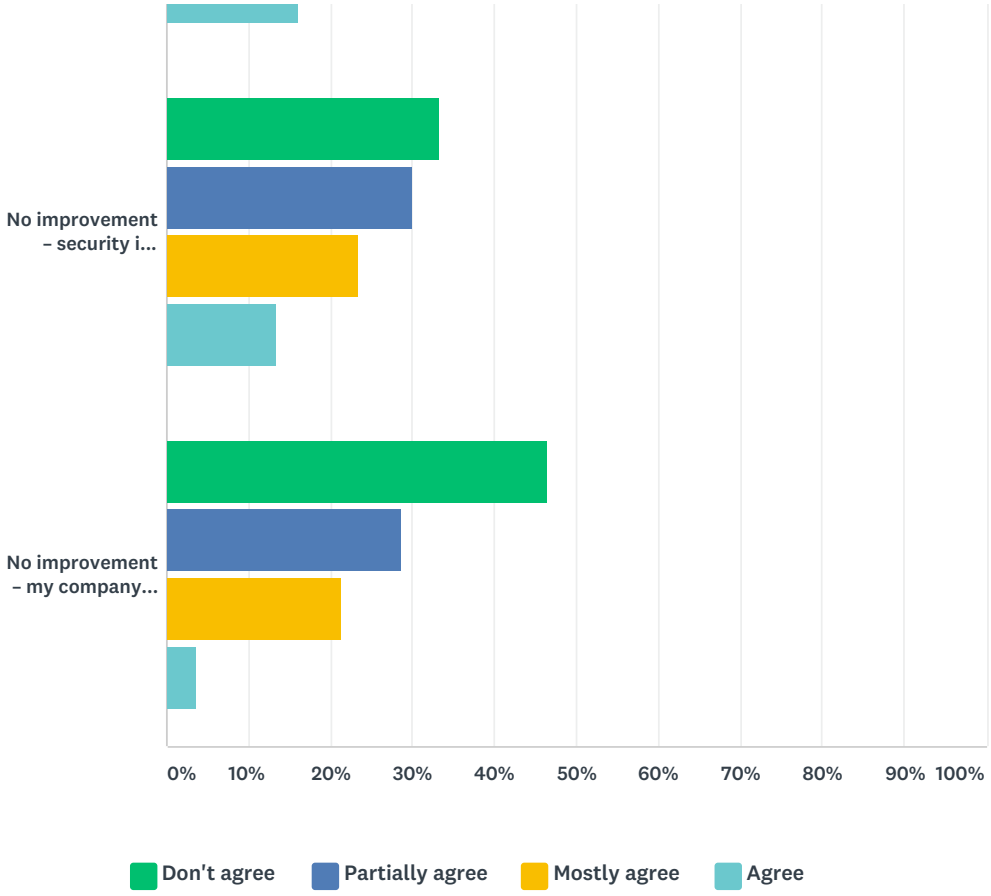


ANSWER CHOICES	RESPONSES	
No	38.46%	15
Yes, my local NDIA chapter	23.08%	9
Yes, my local PTAC and/or NIST MEP Center	25.64%	10
Yes, at an industry conference	35.90%	14
Yes, at Defense Acquisition University	10.26%	4
Yes, from a commercial security training provider	20.51%	8
Yes, from my prime contractor	5.13%	2
Yes, from an internal SME	15.38%	6
Yes, from an external consultant SME	17.95%	7
Total Respondents: 39		

Q35 How much do you believe the DFARS 7012 requirements will help DoD's operational security posture?

Answered: 35 Skipped: 15





	DON'T AGREE	PARTIALLY AGREE	MOSTLY AGREE	AGREE	TOTAL	WEIGHTED AVERAGE
Big improvement – these regulations really improve the overall security landscape to DoD	20.00% 6	46.67% 14	26.67% 8	6.67% 2	30	2.20
Big improvement – In our field, these regulations harden a specific type of vulnerability	24.14% 7	44.83% 13	24.14% 7	6.90% 2	29	2.14
Improvement – there is some uniformity to how much security vendors enact	25.81% 8	51.61% 16	19.35% 6	3.23% 1	31	2.00
Improvement – some security is better than no security	12.90% 4	48.39% 15	25.81% 8	12.90% 4	31	2.39
No improvement – it doesn't matter what vendors do. A determined adversary is going to achieve their goals against DoD	45.16% 14	22.58% 7	16.13% 5	16.13% 5	31	2.03
No improvement – security is getting better, but adversary capabilities got better too	33.33% 10	30.00% 9	23.33% 7	13.33% 4	30	2.17
No improvement – my company's security is better than our customers' security	46.43% 13	28.57% 8	21.43% 6	3.57% 1	28	1.82