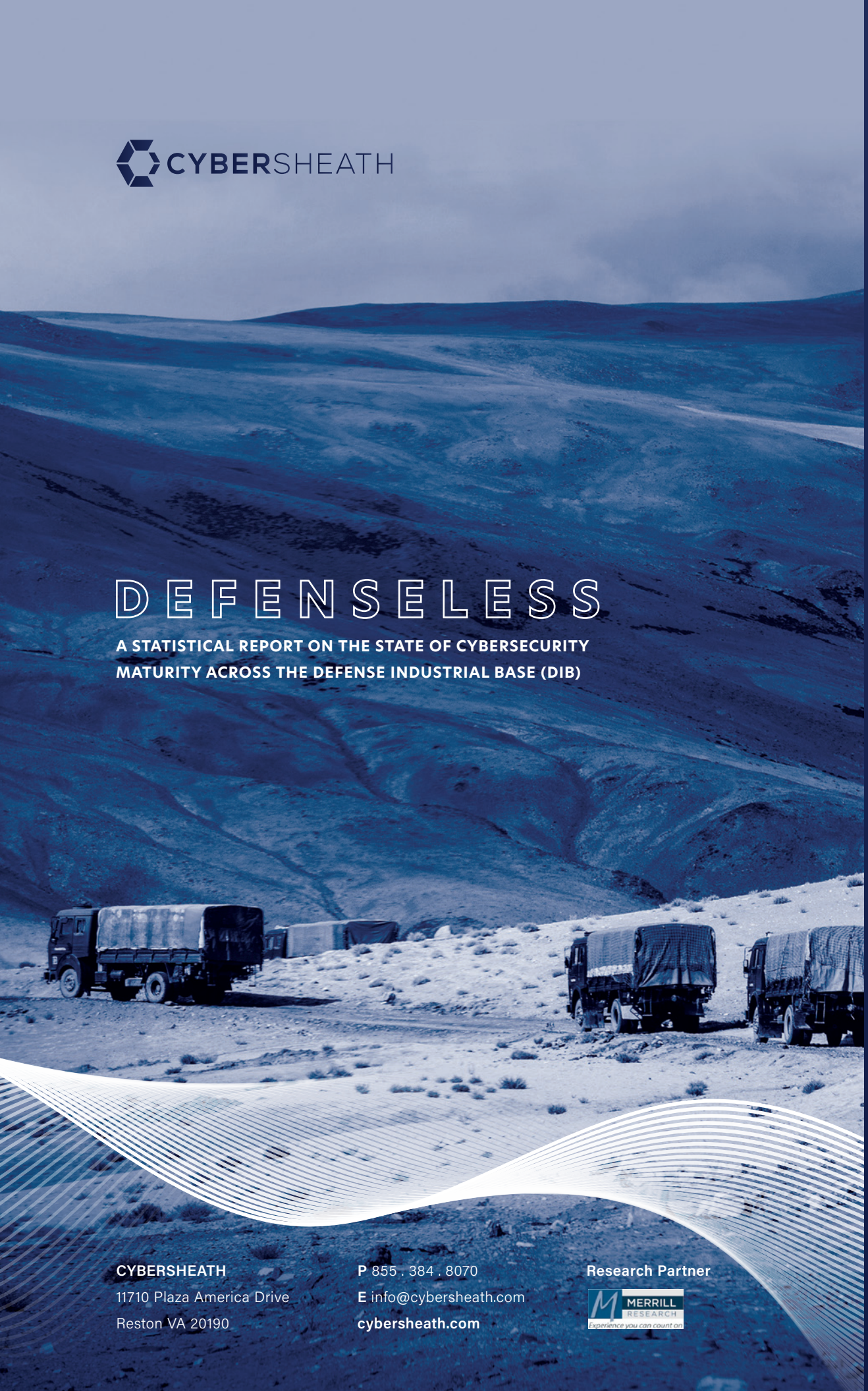
CYBERSHEATH

Cybersecurity Report 2022

DEFENSELESS

A STATISTICAL REPORT ON THE STATE OF CYBERSECURITY MATURITY ACROSS THE DEFENSE INDUSTRIAL BASE (DIB)



CYBERSHEATH
11710 Plaza America Drive
Reston VA 20190

P 855 . 384 . 8070
E info@cybersheath.com
cybersheath.com

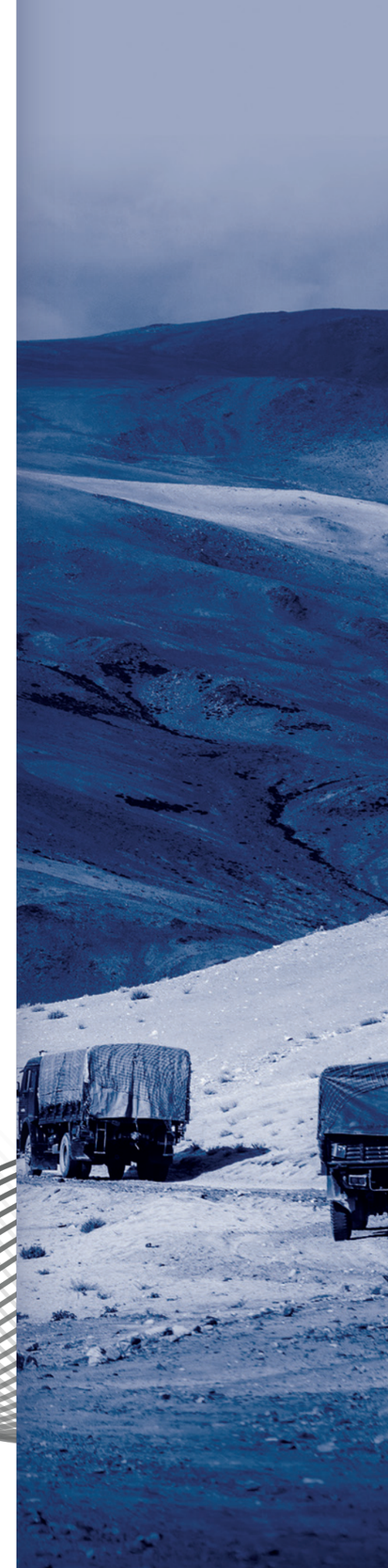
Research Partner

MERRILL RESEARCH
Experience you can count on

CONTENTS

INTRODUCTION

In response to growing concern for the state of cybersecurity across the defense industrial base (DIB) CyberSheath commissioned Merrill Research to conduct a survey of a cross section of the over 300,000 organizations that make up the DIB. The survey targeted 300 individuals responsible for cybersecurity within organizations that are actively seeking CMMC compliance. The data collected provides key insights on where DIB contractors stand in relationship to achieving their CMMC goals, the obstacles facing organizations as they work to achieve and maintain compliance, as well as identifying opportunities for third party support to strengthen cybersecurity efforts.



BASIS FOR THIS REPORT

OBJECTIVE The objective for this study is to gather data to map the progress of cybersecurity maturity across the DIB in the U.S. Market.

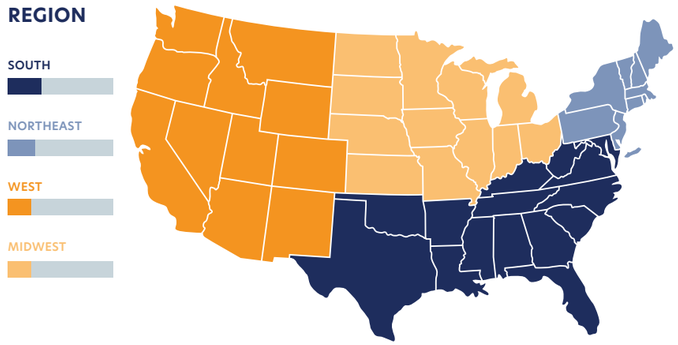
METHOD The data was acquired by online survey and collected in July of 2022

AUDIENCE The audience surveyed as part of this study included 300 individuals throughout the DIB who have a DFARS obligation, are responsible for cybersecurity, and are actively seeking CMMC compliance. To ensure accuracy Merrill also applied the following controls:

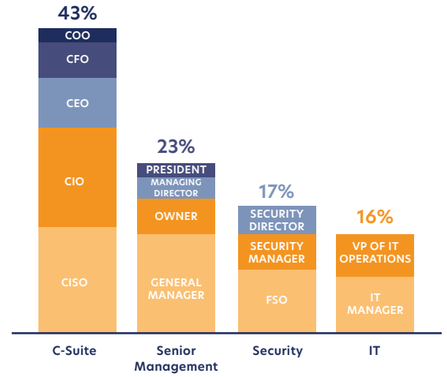
DFARS OBLIGATION	Positive
COMPANY SIZE	10 to 99 Employees
EMPLOYMENT	C-Level / Senior Manager IT / Security

RESPONDENT PROFILE

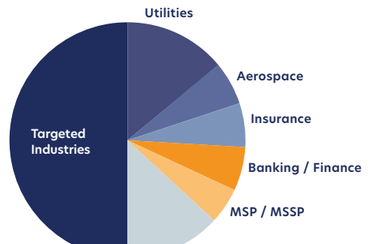
REGION



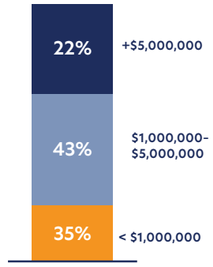
JOB TITLE



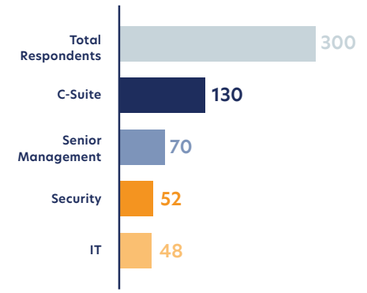
VERTICAL



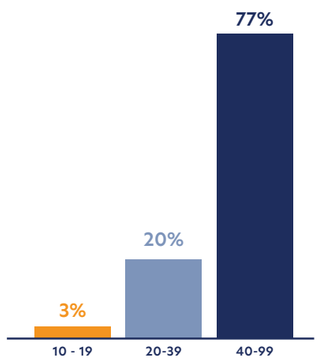
ANNUAL REVENUE



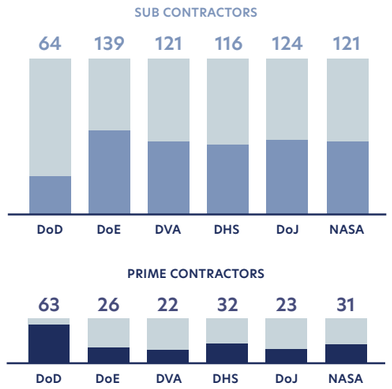
MANAGEMENT ROLE
in number of respondents



NUMBER OF EMPLOYEES
in percentage of respondents



CONTRACT TYPES
in number of respondents



COMPLIANCE RESPONSIBILITY DoD

CYBERSECURITY MATURITY ACROSS THE DIB

While the assumption from the DoD since DFARS Clause 252.204-7012 was enacted in 2017 is that the U.S. is making significant strides toward cybersecurity maturity, the truth is that more than 50% of organizations in the DIB aren't even compliant with the basic DFARS requirements. In fact, this study shows that while 7 in 10 respondents claim to be NIST 800-171 compliant via "self assessment". Only 13% indicated that they have a Supplier Risk Performance System (SPRS) score of 70 or higher. As members of the supply chain that directly supports military efforts, DIB contractor noncompliance poses a direct threat to national security in the United States.

KEY INSIGHTS

Less than 1 in 3 of all respondents have deployed Security Information and Event Management (SIEM).

Only 1 in 5 contractors surveyed have an Endpoint Detection Response (EDR) solution.

Only 1 in 5 respondents reported having an exclusively US based monitoring system.

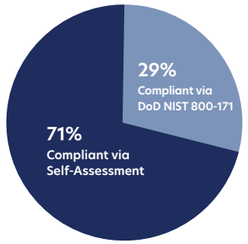
Only 1 in 5 respondents have a plan that includes a Vulnerability Management (VM) solution.

Only 1 in 5 respondents reported having 24/7/365 security monitoring.

Only 1 in 5 respondents have any form of Multi-Factor Authentication (MFA).

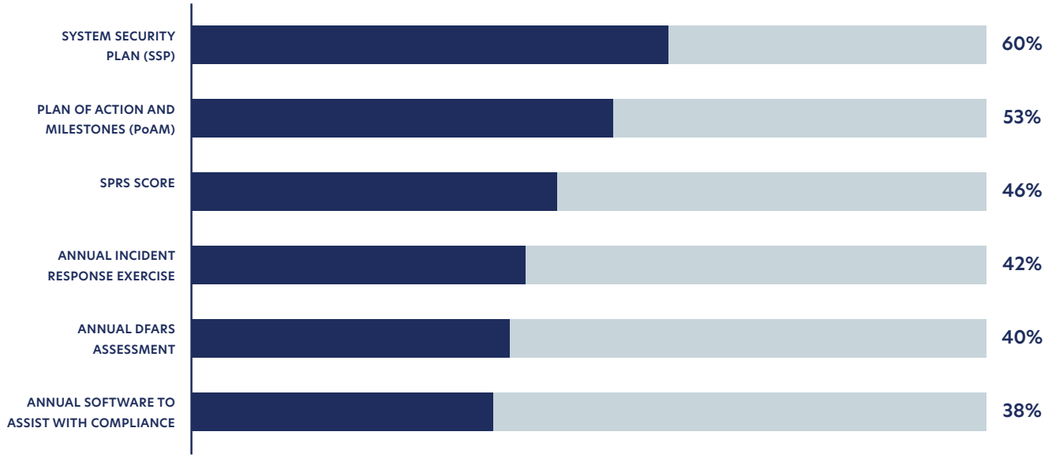
CYBERSECURITY MATURITY

PRIME CONTRACTOR & SUB CONTRACTOR COMPLIANCE WITH DoD NIST 800-171



ALL RESPONDENTS COMPLIANCE WITH DoD NIST 800-171

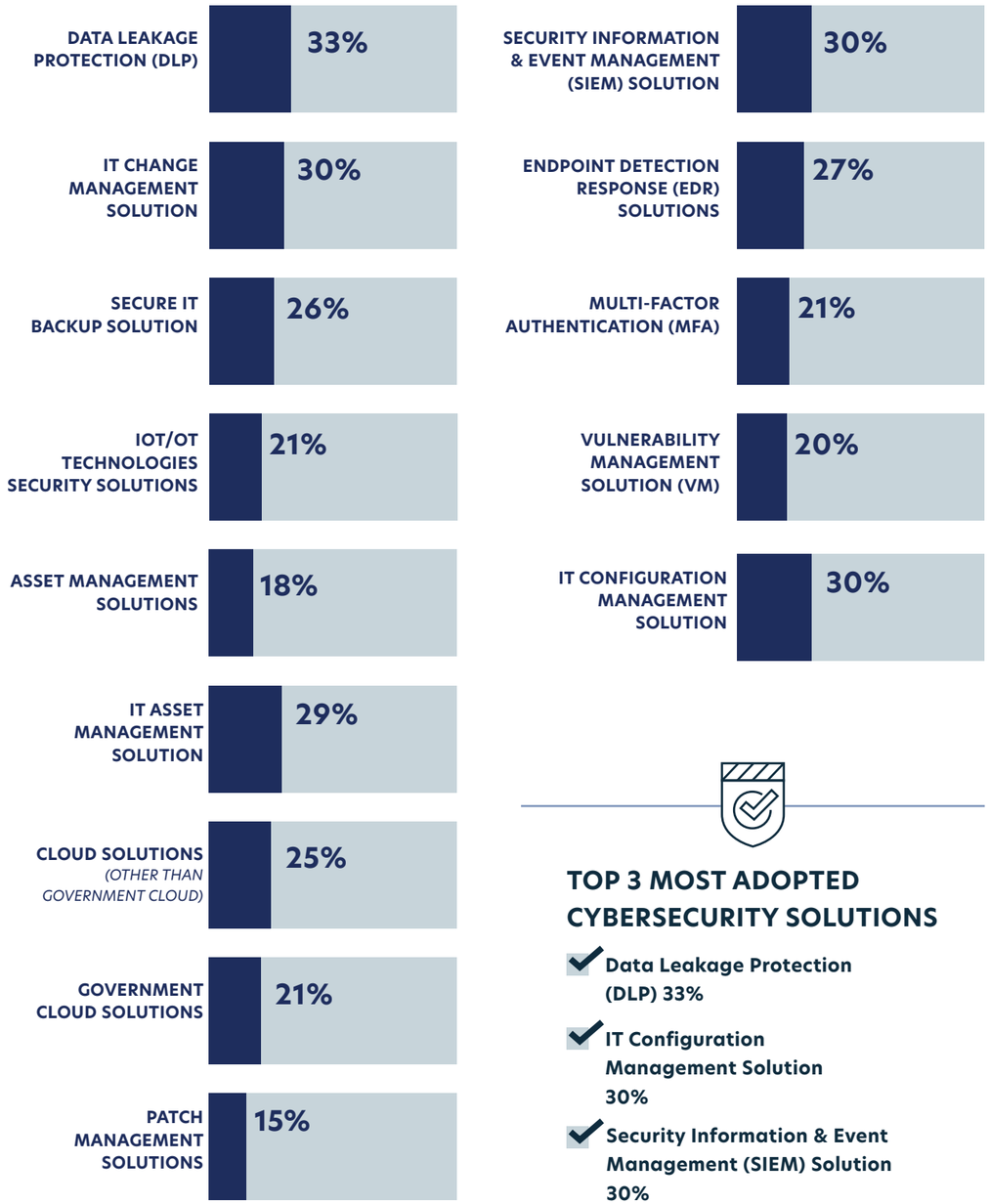
Federal prime contractors and subcontractors that have completed the following elements of DFARS contract obligations



DFARS CONTRACT OBLIGATIONS COMPLETED

CURRENT DEPLOYMENT

All respondents were asked about a variety of solutions. In general adoption is low ranging from 15% at the lowest to 33% at the highest.

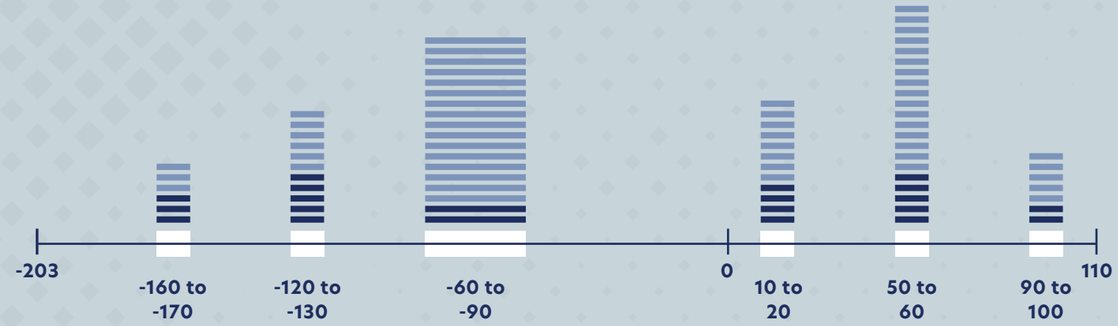


TOP 3 MOST ADOPTED CYBERSECURITY SOLUTIONS

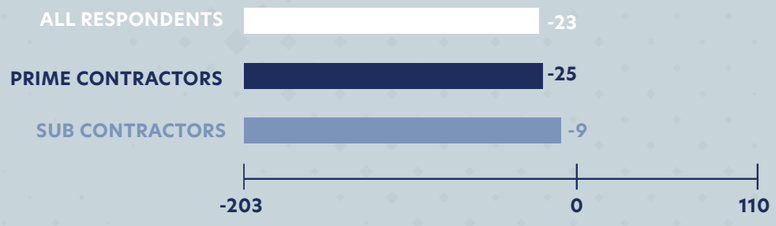
- **Data Leakage Protection (DLP) 33%**
- **IT Configuration Management Solution 30%**
- **Security Information & Event Management (SIEM) Solution 30%**

DFARS CONTRACT OBLIGATIONS

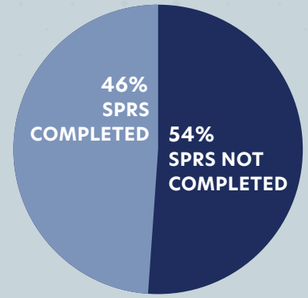
SUPPLIER PERFORMANCE RISK SYSTEM (SPRS) SCORES



SPRS SCORES AMONG RESPONDENTS
in number of respondents



AVERAGE SPRS SCORES



SPRS COMPLETION RATES

What is the Supplier Performance Risk System (SPRS)?

SPRS scores range from a high of 110 (for an organization compliant with all 110 controls) to a low of -203 (for an organization doing none of the NIST 800-171 controls). This study reports that the average DIB contractor has an SPRS score of -23 suggesting significant opportunity for improvement.

OBSTACLES FACING DIB CONTRACTORS IN THE QUEST FOR COMPLIANCE

While compliance is the main topic during any cybersecurity discussion, looming enforcement along with the threat of potential losses have motivated many contractors to set their sights on cybersecurity only to be met by obstacles. When respondents were asked to rate DFARS reporting challenges from 1 - 10 — 10 being extremely challenging — about 60% of all respondents rated “understanding requirements” a 7 in 10 or higher. Also high on the list of challenges was routine documentation and routine reporting.

KEY INSIGHTS

More than 4 out of 5 DIB contractors have experienced a cyber related incident.

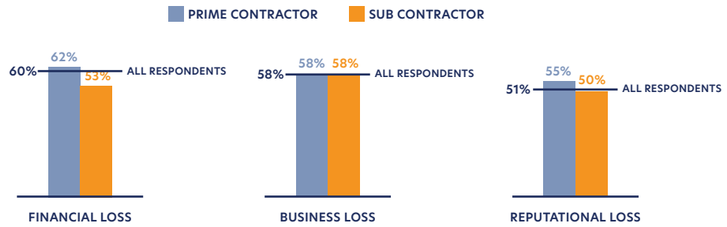
Nearly 3 out of 5 contractors have experienced business loss due to a cyber related event.

More than half of all DIB contractors stand to lose nearly 40% of their revenue if contract loss occurs.

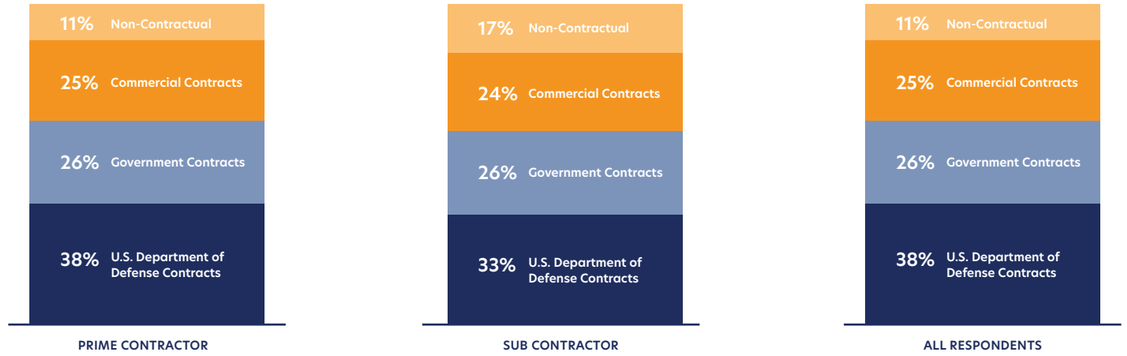
3 out of 5 respondents rate the difficulty of understanding CMMC compliance 7/10 or higher.

Nearly 5 out of 5 respondents have cybersecurity insurance.

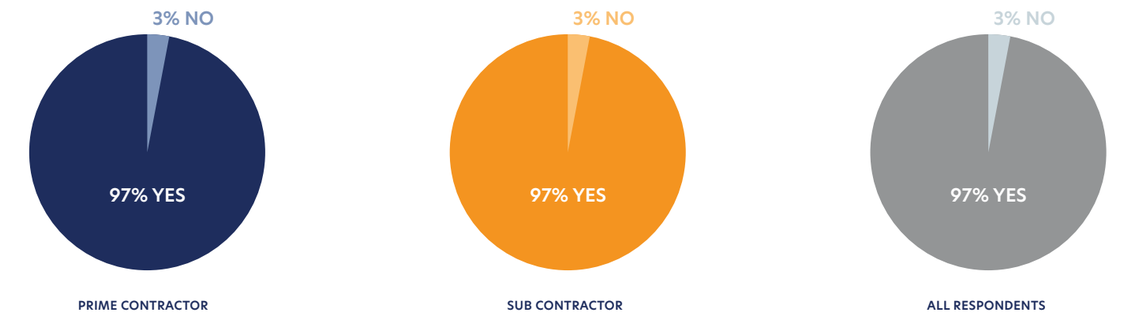
RESPONDENT AWARENESS OF RISK



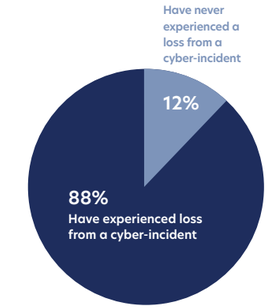
LOSSES EVER EXPERIENCED



REVENUE BY SOURCE

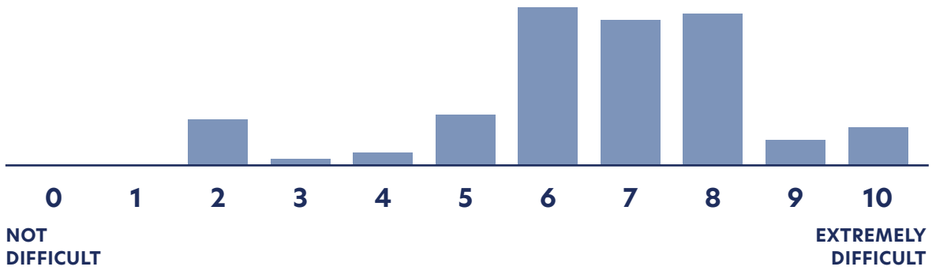


CURRENTLY HOLDS CYBER SECURITY INSURANCE

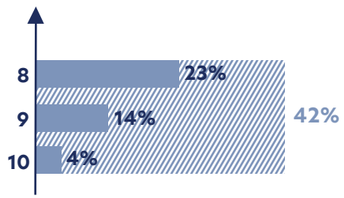


EXPERIENCED LOSS FROM A CYBER-INCIDENT

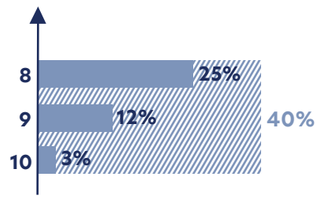
CHALLENGES



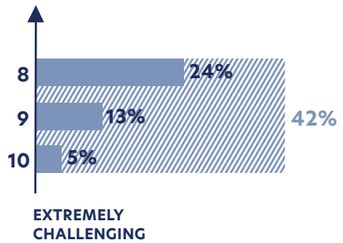
DIFFICULTY UNDERSTANDING HOW TO ACHIEVE / MAINTAIN



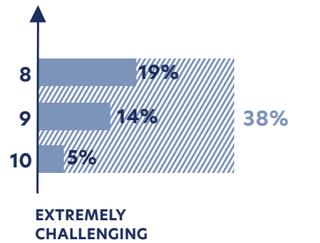
UNDERSTANDING REQUIREMENTS



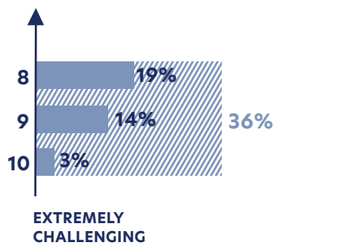
UNDERSTANDING CHANGES



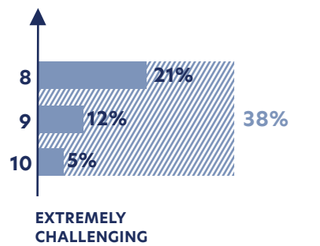
UNDERSTANDING VERBIAGE



ROUTINE DOCUMENTATION



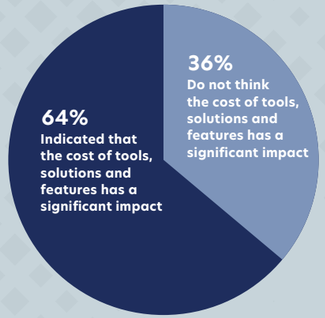
ROUTINE REPORTING



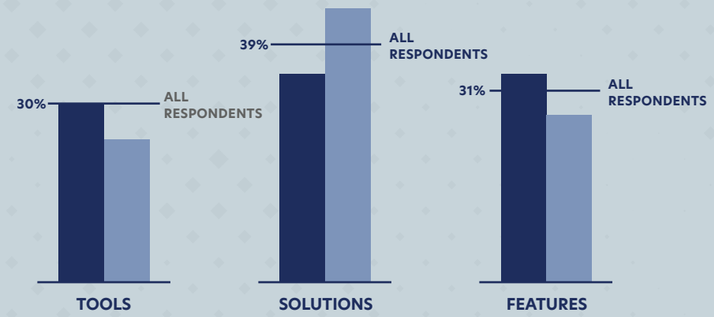
AUDIT SUPPORT

DFARS REPORTING CHALLENGES

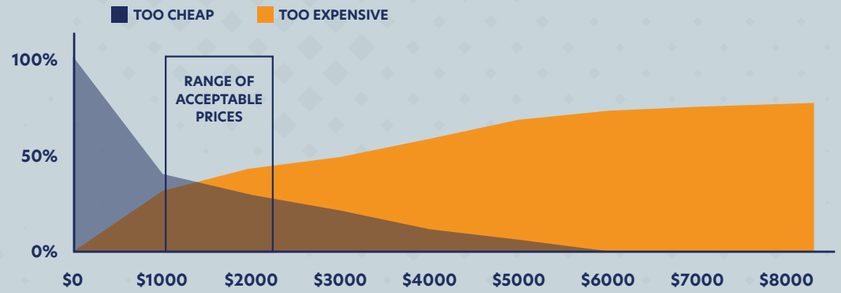
PRICING / COST



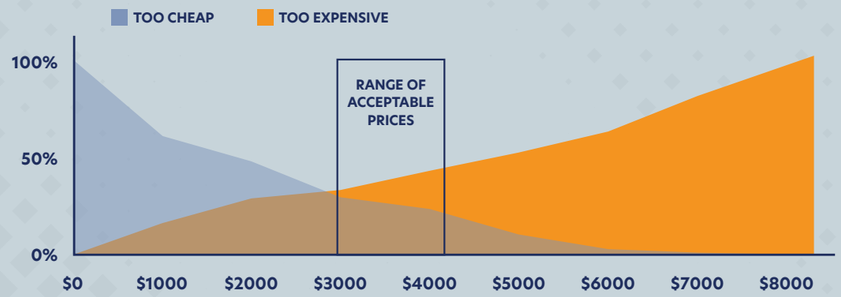
COST OF NEEDED TOOLS, SOLUTIONS & FEATURES ON OVERALL COST



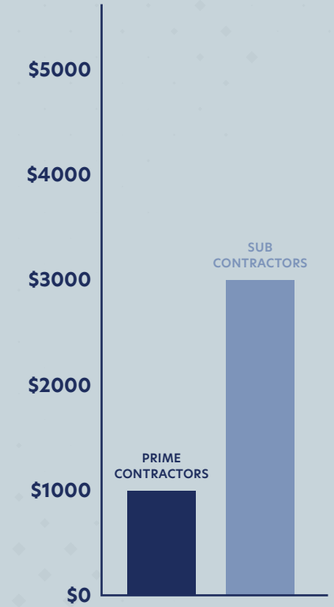
RESPONDENTS RANKING OF HIGHEST IMPACT ON COST



PRICE SENSITIVITY AMONG PRIME CONTRACTORS



PRICE SENSITIVITY AMONG SUB CONTRACTORS



OPTIMUM PRICE POINT AMONG RESPONDENTS

An increase in acceptable prices among sub contractors versus prime contractors plus increased solution deployment rates among sub contractors versus prime contractors suggests a direct correlation between a decrease in price sensitivity and CMMC understanding.

OPPORTUNITIES TO STRENGTHEN CYBERSECURITY EFFORTS

While the state of cybersecurity across the DIB is certainly concerning, this study has identified opportunities for contractors to strengthen their position and build a pathway toward full compliance. As the cybersecurity landscape continues to evolve contractors are becoming more invested in adopting a culture of cybersecurity. This study indicates that about 7 in 10 of all respondents believe that MSPs, MSSPs and technology providers should be certified, and nearly 50% of contractors believe DFARS improvements have a significant impact on national security overall. The key to achieving cybersecurity maturity will depend on building pathways to effective and sustainable solutions, and continuing to increase the understanding of those responsible for CMMC compliance across the DIB.

KEY INSIGHTS

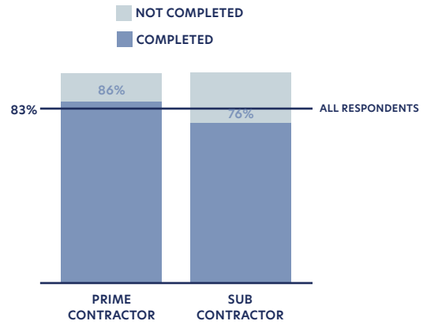
Nearly half of all respondents think DFARS improvements have a significant impact on national security.

Of the respondents with POAMs nearly half have not completed their documentation.

More than 3 out of 5 respondents believe MSPs, MSSPs, and IT providers should be certified.

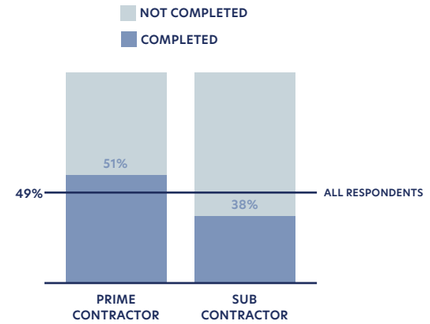
More than 4 out of 5 respondents have completed an assessment of their current operations for compliance with NIST 800-171.

DFARS STEPS COMPLETED



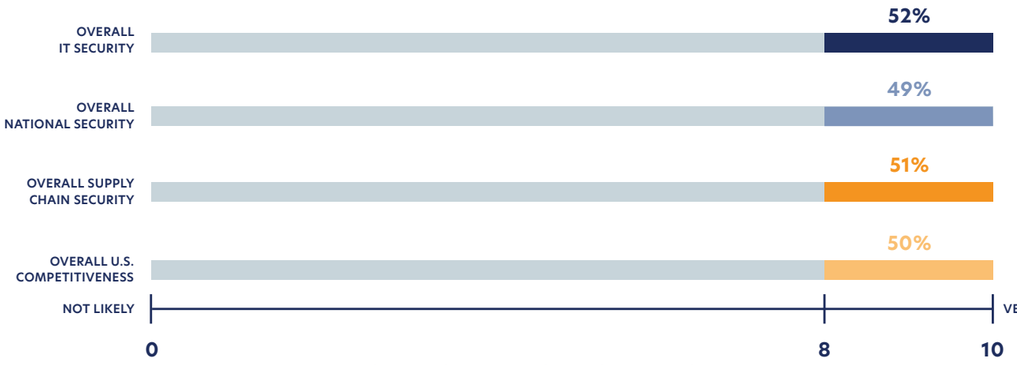
ASSESSMENT OF CURRENT OPERATIONS WITH COMPLIANCE WITH NIST 800-171

in percentage of respondents



PLANS FOR ONGOING COMPLIANCE (POAMs)

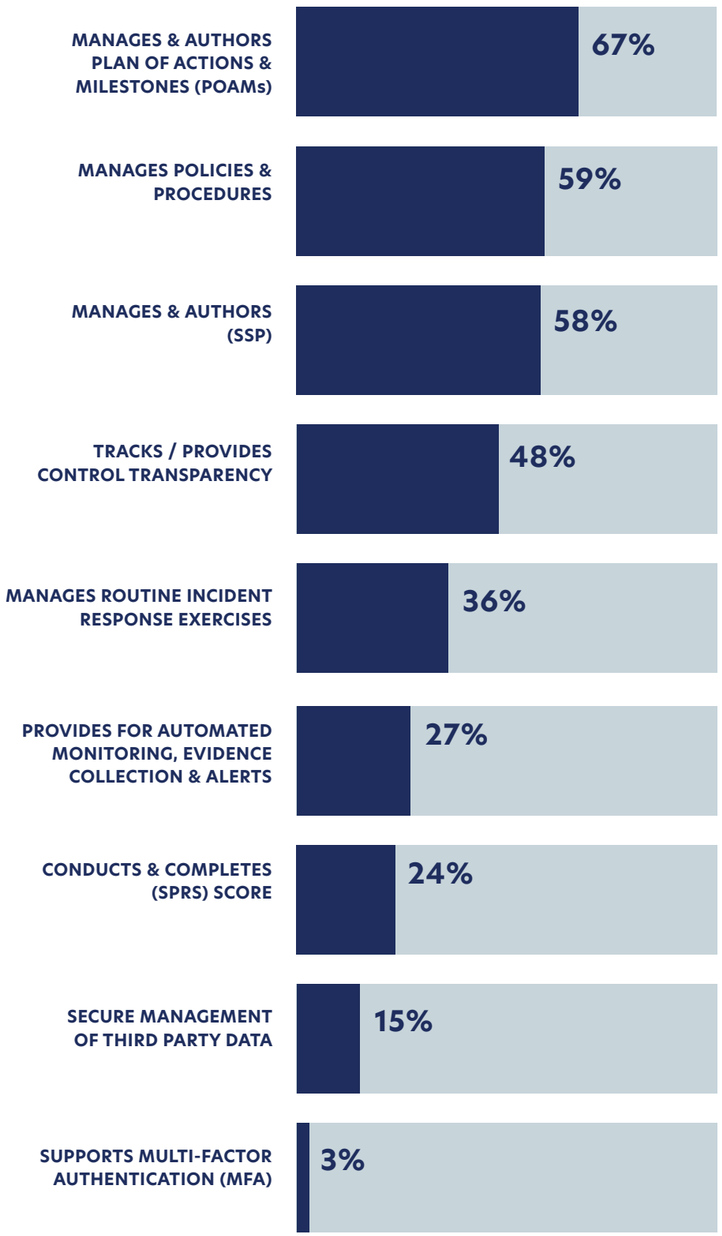
in percentage of respondents



DFARS IMPROVEMENTS PERCEIVED TO HAVE A SIGNIFICANT IMPACT

WHO SHOULD BE DFARS CERTIFIED

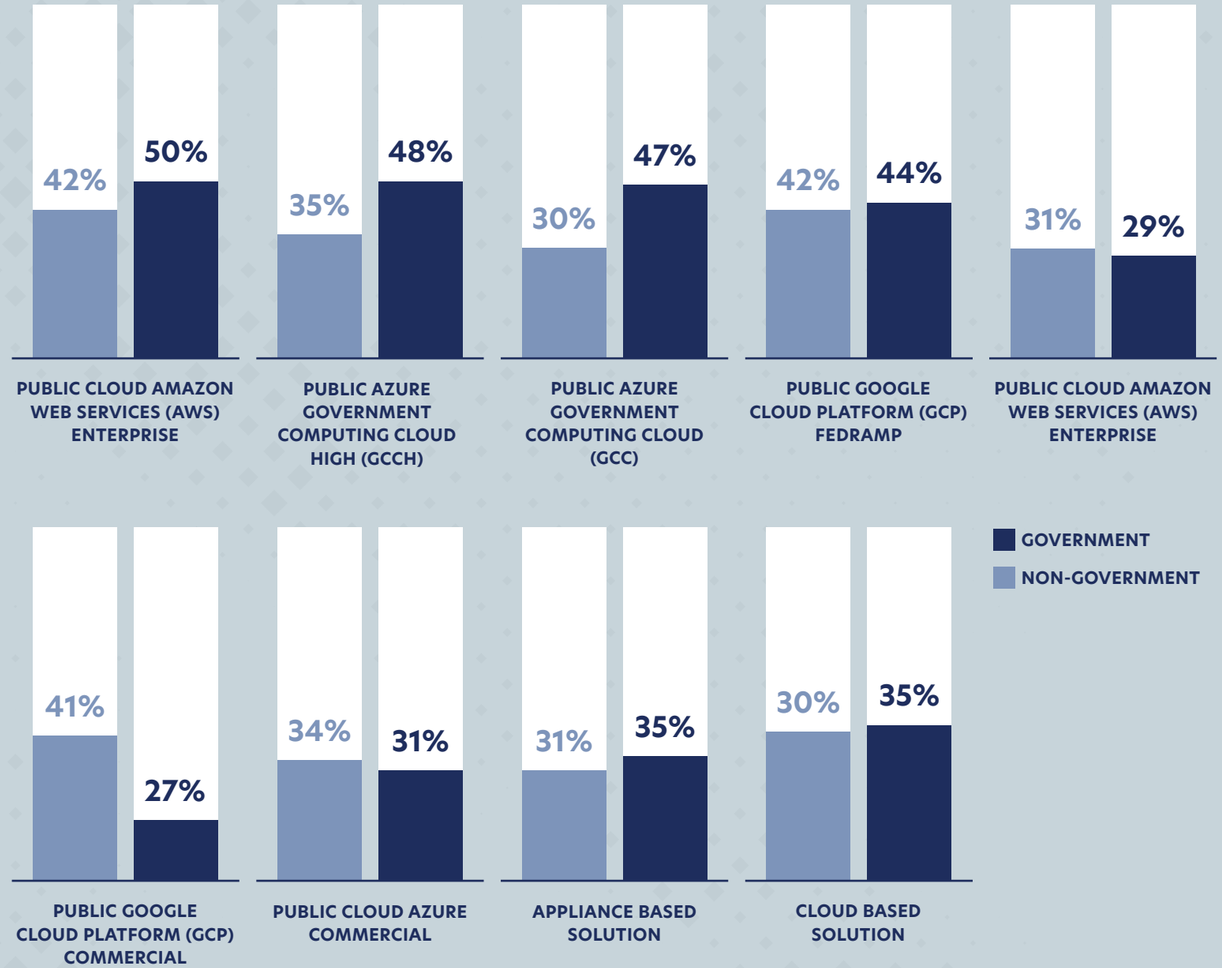
AVAILABLE SOLUTIONS



DEPLOYMENT OF SOFTWARE SOLUTION TO ASSIST WITH COMPLIANCE AMONG RESPONDENTS

CLOUD SOLUTIONS

Of the 300 respondents 25% indicated they have non-government cloud solutions to assist with compliance while 21% indicated they have government cloud solutions.



RESPONDENTS WHO DEPLOY CLOUD SOLUTIONS USE

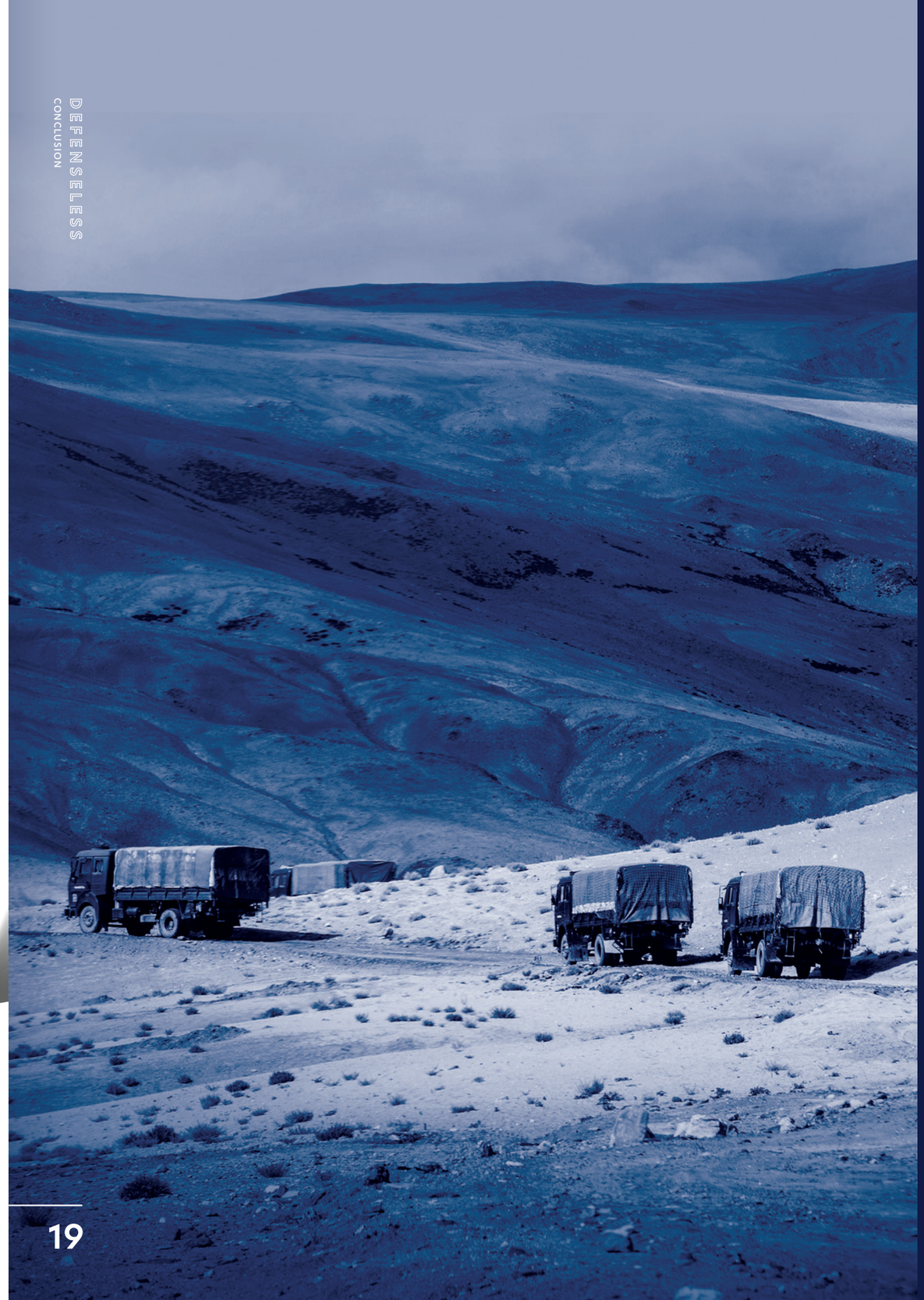
TOP 3 MOST DEPLOYED GOVERNMENT CLOUD SOLUTIONS

Among those currently deploying government cloud solutions, Azure is the largest cloud solution provider, followed distantly by AWS then Google Cloud.

- Azure 84%
- AWS 66%
- Google Cloud 61%

CONCLUSION

Many contractors across the DIB still struggle to achieve and maintain CMMC compliance. The primary obstacles in this effort are the difficulty understanding the necessary steps to achieve compliance, the difficulty implementing sustainable CMMC policies and procedures, as well as overall cost. As the DoD becomes increasingly dependent on technology, cyber attacks continue to escalate — both in frequency and proficiency. The good news is that DIB contractors are more invested than ever in adopting a culture of cybersecurity as a matter of duty and are looking to CMMC as a guide. As the cybersecurity landscape continues to evolve it is our responsibility to continue to advocate for third-party certification, build pathways to effective and sustainable solutions, and increase the understanding of CMMC within the DIB overall.



NEXT STEPS

A PORTRAIT OF FULL COMPLIANCE

How will it look when your organization achieves full compliance? Through our years of front line experience supporting organizations in the DIB, we have observed three critical characteristics.

SHARED RESPONSIBILITY

Make sure that ownership for compliance never rests with a single department, employee, or vendor. Instead, manage it as a shared responsibility and document the interdependent accountabilities. This documentation is critical to success.

INTEGRATED PEOPLE, PROCESSES & TECH

Don't focus so much on licensing and technology that you lose sight of the bigger compliance picture. Aim to strike the right balance across these three vital resource areas.

CONTINUOUS COMPLIANCE

Don't want to slip into non-compliance? Make sure you are continuously auditable by validating your approach monthly, quarterly, and annually. Use a programmatic approach to ensure alignment with requirements.

In a well-designed program, you will naturally discover and remediate gaps in operational or compliance capabilities. Issues and challenges are an expected part of your program – and you have clear ways of handling them.

WHY WORK WITH CYBERSHEATH?

EXPERIENCE

The CyberSheath team is distinguished by our DFARS/CMMC expertise. In fact, our executives have been involved in the development of every major DoD cybersecurity initiative since 2008. Since our founding in 2012, we have completed more than 600 NIST 800-171 assessments and solutions for our clients.

FOCUS

Cybersecurity compliance is all we do. As one of the industry's only one-stop providers, we help our clients solve the whole problem. We tell you exactly what you need to be compliant – and then we deliver it.

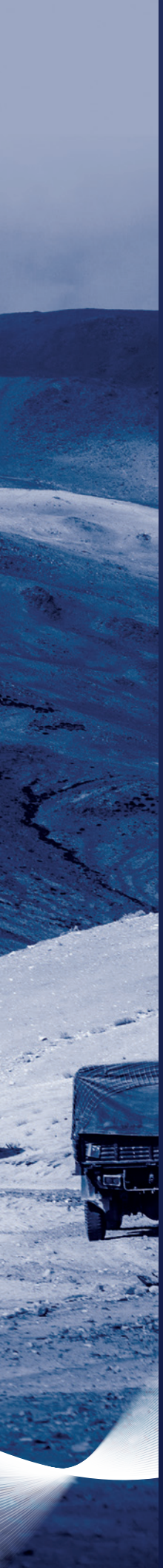
EFFICIENCY

With CMMC 2.0, noncompliance will be a deal breaker. CyberSheath has time-tested methods and tools for helping your organization achieve and maintain full compliance with all applicable DoD requirements. We can show you how to achieve compliance at the appropriate level, with a minimum amount of pain.

Need Help?

Do you want to understand where you stand in your DFARS journey compared to the DIB? Contact us to discuss your specific situation to learn how we can help.

CYBERSHEATH



CYBERSHEATH

CYBERSHEATH
11710 Plaza America Drive
Reston VA 20190

P 855 . 384 . 8070
E info@cybersheath.com
cybersheath.com

Research Partner

MERRILL RESEARCH
Experience you can count on