BEYOND OBFUSCATION:

The Defense Industry's Position within Federal Cybersecurity Policy

A Report of the NDIA Policy Department

PROJECT DIRECTORS

Corbin Evans
Christopher Smith

October 2019

ABOUT NDIA

The National Defense Industrial Association drives strategic dialogue in national security by identifying key issues and leveraging the knowledge and experience of its military, government, industry, and academic members to address them.

NDIA, comprised of its Affiliates, Chapters, Divisions, and 1,600 corporate and 85,000 individual members, is a non-partisan, non-profit, educational association that has been designated by the IRS as a 501(c)3 nonprofit organization—not a lobby firm—and was founded to educate its constituencies on all aspects of national security.

NDIA formed from a merger between the American Defense Preparedness Association, previously known as the Army Ordnance Association, founded in 1919, and the National Security Industrial Association, founded in 1944. For 100 years, NDIA has provided a platform through which leaders in government, industry, and academia can collaborate and provide solutions to advance the national security and defense needs of the nation.

DISCLAIMER

ACKNOWLEDGEMENTS

This project would not have been possible without the combined efforts of the NDIA Policy and Strategy teams. NDIA would like to thank the following individual contributors: Alex Berge, Hannah Harper, Zach Kronisch, and Mike Patterson

EXECUTIVE SUMMARY

The adoption and deployment of cyber technologies have improved the effectiveness of U.S. warfighters across the globe. From reducing the cost of and lead-time for high-tech weapons production to ensuring reliable communications across the battlefield, cyber underlies many defense innovations.

However, despite the numerous advantages of a cyber-connected world, the proliferation of cyber tools presents an array of threats and vulnerabilities that deserve the attention of decision-makers across the defense enterprise. Cybersecurity breaches are increasingly common across industry and government, with the defense industry being no exception. As the cost of these breaches reaches into the billions of dollars, demand for more robust cybersecurity controls and regulations comes from the highest levels of government and Congress.

Cyber policies directed at the defense industrial base are continually evolving and increasingly complex. New and established actors are facing challenges regarding the adoption of and compliance with policies disseminating from Congress and the Department of Defense (DoD). Ensuring members of the defense industrial base take the threat of cybersecurity seriously, understand policies, and are adequately fortified against would-be cyber adversaries is a priority throughout the defense community. NDIA—as the go-to convener of industry, academia, and government—stands at a unique position to educate industry while also communicating industry's views to government.

The *Beyond Obfuscation: The Defense Industry's Position within Federal Cybersecurity Policy* report illustrates the risks and vulnerabilities within the cyber domain for the defense industry, educating industry about the evolution of cyber regulations while communicating to the defense community the views of industry.

SECTION I: ILLUSTRATIONS OF CYBER THREATS AND VULNERABILITIES

Throughout the past decade, the global cyber threat level has intensified, subjecting private industry and government alike to an increasing flurry of cyber-related attacks. These intrusions have not only grown in frequency but also in severity as they are now responsible for billions of dollars lost each year. Both state-sponsored and private-actor attacks are on the rise across the globe, grabbing the attention of both the media and policymakers. Despite private industry's reluctance to share news of intrusions into their networks, we now have a plethora of examples illustrating the range of attacks that have occurred.

In this section, case studies of past marquee cyber incidents present lessons alongside more recent examples, demonstrating the pervasive and varied nature of cybersecurity breaches. Each event either demonstrates a new avenue of intrusion or illuminates a previously unknown vulnerability. Culminating in a presentation of the *Threat Matrix*, a framework breaking down attacks using the *cyber kill-chain method of analysis*, these cases are meant to communicate to industry that no individual actor is immune from cyber threats.

SECTION II: POLICY RESPONSE TO CYBER RISK

As the cost and severity of cyber attacks increase, government has scrambled to develop solutions. Federal, state, and local policymakers have exercised a myriad of policy responses to shore up public and private cybersecurity fortifications, covering a range of executive and legislative actions. Often driven by the perceived need to respond to high-profile cyber incidents, these responses are often spurious and fragmented. Though well-meaning, prescriptive documents like the U.S. National Cyber Strategy propose a broad but lightly specified whole-of-government approach to reducing cyber risk while implementing agencies fall short of adequately hardening government assets, operations, and tools against attacks.

Those in the defense industrial base are left to wade through a complicated, multi-layered set of policy regulations that feature separate authorities and conflicting institutional agents. Intimidating to even the most established of defense contractors, this odious regulatory environment is a worrisome barrier to entry and a major deterrent to better cybersecurity practices. Summaries of the regulatory authorities most directly responsible for such an environment are presented to disentangle and demystify the new wave of cyber regulations. At a time when the Department of Defense aims to roll out a new draft policy through the Cybersecurity Maturity Model Certification (CMMC), understanding where we are is essential to comprehending where we are going.

SECTION III: INDUSTRY'S PERSPECTIVE (SURVEY ANALYSIS)

Any discussion of the effectiveness of the policy response to cyber threats is incomplete without the perspective of the defense industrial base. Often serving as the first line of defense and the subject of new and existing regulations, members of this group are uniquely qualified to evaluate the current state of affairs. A survey instrument was developed and deployed to ferret out industry's perspective. Questions were included to measure the financial impact of cyber policy compliance, to determine industry's cyber hygiene best practices, and to clarify industry's opinion on current cyber regulations.

The survey's results measured notable differences in experiences between large and small companies, prime contractors and subcontractors, and new entrants and established actors.

Key Findings:

- More than 25 percent of industry professionals work for firms that have experienced a cyber attack
- 44 percent of companies with more than 500 employees have experienced a cyber attack
- Industry views cyber attacks from outside actors as the most serious cyber threat, followed closely by the threat of a cyber attack by a former employee
- Small companies use security measures such as firewalls and multi-factor authentication at a much lower rate than large companies
- Companies are only marginally confident in their ability to recover from a cyber attack within 24 hours
- 30 percent of companies do not have a good sense of the cost needed to recover from a cyber attack
- Small businesses are 15 percent less likely than large businesses to agree with the statement that "our employees are well prepared to understand and respond to cybersecurity threats"
- 72 percent of large businesses agreed they were prepared to comply with DFARS 7012 requirements, but only 54 percent of small businesses agreed
- 44 percent of prime contractors have not been able to verify their subcontractors' system security plans

SECTION IV: CONCLUSIONS AND RECOMMENDATIONS

Recommendations for Government

Increased communication, right-sizing the flow of information, and simplifying the current cyber regulatory regime are the first steps that government should take to increase the operational security of the defense industry. A disparity exists between large, established actors and smaller businesses on cyber awareness, preparedness, and compliance. Small businesses need targeted government communications and resources to ensure that they remain a part of the industrial supply chain. New policies must also consolidate regulatory authorities to decrease the compliance burden on industry while accounting for the current experience and expertise of industry partners during policy development.

Recommendations for Industry

Industry must be equally committed to solving the issue of cyber breaches as government. As the source of much innovation relied on to improve the capabilities and lethality of the warfighter, industry must be ready to protect the innovative technologies for which they are responsible to develop. Prime contractors must be willing to share best practices and experiences with lower-tier, more unexperienced companies while working with government to manage the flow of sensitive information within the supply chain. Smaller businesses need to make a more intentional effort to adopt cyber fortifications and ensure compliance with current cyber regulations meant to increase their level of security. All of industry must commit to working with government as the new CMMC program is developed to ensure that the new set of regulations is as effective as possible without an unduly burden on industry.

CONTENTS

INTRODUCTION

Cybersecurity has surged to become an urgent government-wide concern as organizations both public and private struggle to reduce their exposure to cyber attack risk exposure. As massive cyber breaches of large corporations and governments alike make headlines policymakers respond with new programs and policies designed to reduce vulnerable targets. As a result, the defense acquisition community enters a new era of adaptation and adjustment to an emerging regime of cybersecurity requirements. For industry, however, a great deal of uncertainty persists regarding both existing requirements and newer guidelines.

How should defense industry executives understand their unique risk in terms of threats and vulnerabilities? What is the government's strategy for reducing cyber risk, and what are the implications for industry? What best practices for addressing cyber risk has the defense industrial base produced? This report attempts to answer these questions and provide a guide to the state of industry's cyber-defense readiness by synthesizing the latest published expertise on the cybersecurity challenges facing the defense industrial base, analyzing federal cyber strategy and policy, and presenting original evidence of emerging defense sector attitudes toward the emerging defense acquisition cybersecurity policy regime.

This project offers something for the most read-in policy experts in addition to new entrants to the federal marketplace seeking an introduction to the issue of cybersecurity. The survey presented in Section III provides a snapshot description of cybersecurity behavior, attitudes, and preferences drawn from a representative sample of the defense industrial base. Developed in conjunction with the NDIA San Diego Chapter, our research offers unique insights into industry's experience with cybersecurity.

Aimed at informing not only a beltway policy audience, but also industry peers and academic researchers, we present the findings of this study with the hope that we can further reduce the threat that cyber attacks pose to our national security. Industry's current actions and perceptions of the threat must be taken into account by regulations to achieve the stated goal of increased security.

SECTION I: ILLUSTRATIONS OF CYBER THREATS & VULNERABILITIES

Rarely do we go more than a day without a disturbing new cybersecurity event on the front page of the newspaper. As the frequency and severity of these attacks increase, so must our examination and understanding of the methods of attack and where these attacks are being targeted. However, corporate and government leaders too often obfuscate or avoid announcements revealing network cyber intrusions. This lack of transparency lessens our ability to achieve a comprehensive understanding of the threat. Secrecy not only hinders threat assessment, but also stymies efforts to devise and implement counter measures.

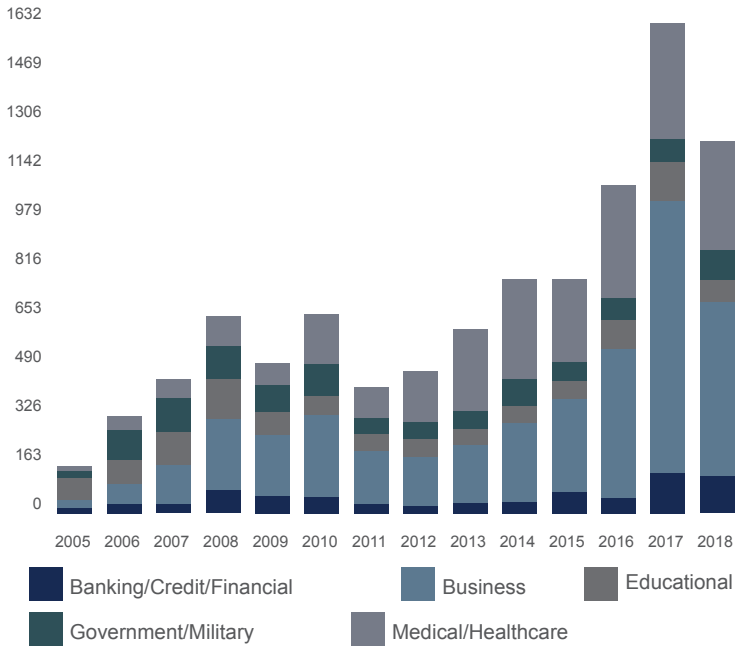
These limitations notwithstanding, in this report, we provide an overview of the current state of threats to industry in the cyber domain, including description of frequent methods of attack. The vignettes provided herein illustrate real-world dynamics of how malicious actors take advantage of insecure private and government information systems, costing taxpayers and investors millions of dollars. Marquee breaches over the past several years demonstrate the variety of targets, attack vectors, exploits, and vulnerabilities that adversaries employ. We present case studies of several of such breaches to provide a brief, defense industry-oriented survey of attackers' methods and victims' vulnerabilities, as well as the potential consequences, financial and otherwise, of such incidents. The defense industry has proven to be uniquely attractive to cyber adversaries. Often responsible for safeguarding our nation's most highly guarded secrets, the defense industry has already experienced many damaging cyber attacks and all signs point to the continuation of this trend.

STATISTICS SNAPSHOT OF 2018

Security breaches are an inherent risk of the internet's open architecture. As a result of the rapid global expansion of Internet access, such breaches have increased exponentially. Reported breaches have reached record numbers – so far in 2019, attacks have increased by 54%.[1] As shown in Figure 1, since 2005, total reported data breaches increased from fewer than 250 to approximately 1,250 as of 2018. Industry-targeted attacks have been the main contributor to the increase. Moreover, these attacks entail costs greater than data and intellectual property loss, including costs associated with recovering stolen data, repair of damaged systems, and lost economic opportunities for trade and commerce. The impact of these breaches on the U.S. economy is difficult to measure but almost certainly substantial.

1 Sanders, James, "Data breaches increased 54% in 2019 so far," TechRepublic.com, August 15, 2019. Url: https://www.techrepublic.com/article/data-breaches-increased-54-in-2019-so-far/. Last accessed: September 26, 2019.

FIGURE 1: DATA BREACHES BY YEAR[2]



These attacks impose a substantial negative economic impact. In 2018, the Poneman Institute, an independent research agency, found the average total cost of a data breach to be $3.92 million globally.[3] The United States led the way with the most expensive average data breach cost at $8.19 million, with an average of 25,575 records lost per breach. Cyber incidents falling into the "mega breach" category result in the loss of 50 million or more records, rising to $350 million in average total cost.[4] The Poneman study also found that costs associated with breaches are on the rise compared to 2017, with the average total cost of a breach having risen 6.5 percent.[5] Poneman also noted a 2.2 percent increase in the overall size of data breaches from 2017 to 2018.[6]

The Senate Permanent Subcommittee on Investigations paints an even bleaker picture of today's cyber threat environment, showing that important public data is also at risk. According to a committee staff report released in 2016, cyber attacks on federal agencies have increased by 1,300 percent from 2006 to 2015. Cyber criminals exploit the federal government's reliance on legacy IT systems laden with cybersecurity risk. These systems often use both outdated software and hardware, making them easy targets for advanced cyber attacks.

A SNAPSHOT OF RECENT ATTACKS

2018 showed that not all cyber attacks are alike. The cyber attacks that dominated the year's news cycles included a range of target types and attack vectors, such as breaches of personal data, hacks of educational and government institutions, private companies, and social media platforms. Not least, such attacks have the ability to impact every part of our daily lives, because no public or private organization with a computer network is immune.

Equifax

No recent breach attracted more public attention than the hack of Equifax. One of three major consumer credit rating agencies, Equifax disclosed in late 2017 that attackers had breached its data archives, obtaining sensitive personal information including names, birth dates, Social Security numbers, addresses, and driver's license numbers of 147 million customers. For approximately 209,000 customers, the breach exposed also credit card information. The firm reached a $425 million settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau, and all 50 states in 2019.[7]

Marriott

Not even the world's largest hotel company could protect itself from cyber disaster.[8] In September 2018, Marriott hotels announced it had suffered a massive data breach affecting nearly 400 million customers to theft.[9] The breach started in 2014 and unfolded over years with attackers stealing contact information, passport numbers, arrival and departure dates, and reservation information. This breach represents one of the largest in history.

Facebook

Neither has tech giant Facebook been secure from data theft. Over 30 million Facebook accounts were hacked in late 2018.[10] The perpetrators stole Facebook "access tokens" and used them to take over the accounts of other people. 15 million people had personal information stolen.

Universities

American universities have also fallen victim to state-sponsored cyber attacks. In March 2018, the U.S. government charged nine Iranians with stealing data and intellectual property from 300 domestic and foreign universities over a three-year period.[11] Reports estimate more

2 "2018 Annual Data Breach Year-End Review." Identity Theft Resource Center. Cyber Scout, 2018. https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf.

3 Poneman Institute. "Cost of a Data Breach Report." IBM Security, 2019. https://www.ibm.com/security/data-breach.

4 Ibid.

5 The Poneman Institute used four factors in calculating the cost of a data breach: loss of customers as a result, the size of the breach, the amount of time taken to identify and contain it, and effective management of detection and post-breach costs.

6 Ibid.

7 Equifax. "Equifax Announces Cybersecurity Incident Involving Consumer Information." Equifax, September 7, 2017. https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628. ;"Equifax Data Breach Settlement." Federal Trade Commission, September 9, 2019. https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement.

8 Touryalai, Halah,"World's Largest Hotels 2018: Marriott Dominates, Hyatt & Accor Rise," Forbes.com, June 6, 2018. https://www.forbes.com/sites/halahtouryalai/2018/06/06/worlds-biggest-hotels-2018/#4e62058f47c7 [Last accessed: September 26, 2019]

9 Security and Exchange Commission. "Marriott Announces Starwood Guest Reservation Database Security Incident," November 30, 2018. https://www.sec.gov/Archives/edgar/data/1048286/000162828018014745/a2018ex99.htm.; Starwood Resorts. "Starwoods Response to Breach," March 4, 2019. http://starwoodstag.wpengine.com/wp-content/uploads/2019/05/us-en_Second-Response.pdf.

10 Facebook, Inc. "Security Update." Facebook Newsroom, September 28, 2018. https://newsroom.fb.com/news/2018/09/security-update/.; Rosen, Guy. "An Update on the Security Issue." Facebook Newsroom. Facebook, Inc., October 12, 2018. https://newsroom.fb.com/news/2018/10/update-on-security-issue/.

11 United States Department of Justice. "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps." The United States Department of Justice, March 23, 2018. https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-

than 31 terabytes of information worth more than $3 billion worth of intellectual property. The attackers used "spear-phishing" attacks to obtain login information of university staff. More than 100,000 professors were targeted while 8,000 accounts were successfully infiltrated—almost half of which were accounts at U.S. schools. The alleged culprits are still believed to be in Iran.

VPNFilter

Neither has consumer electronics hardware gotten a pass from cyber crime. In May 2018, cybersecurity experts called attention to the growing threat from VPNFilter, a new and sophisticated malware targeting popular makes and models of home and small office networking routers.[12] Once infected, the malware siphons data from the users, collecting credentials and other user information. VPNFilter, which infected over 500,000 routers inside Ukraine after its initial release, has been traced to hackers working under the direction of the Russian government.[13]

LESSONS FROM MAJOR PAST CYBER ATTACKS

The previous examples are snapshots of the larger cybersecurity landscape, in which cyber threat levels are rising for government and industry. As cyberspace has grown as a commercial medium and tool of service delivery and manufacturing, so too has the number of attack vectors available to malicious actors. Nonetheless, the form of most cyber attacks aligns with certain archetypes. The following section uses high-profile cybersecurity breaches to depict major types of cyber attacks, spanning a range of attack vectors and targets. These selected examples, which represent some of the most destructive and most infamous cyber attacks of our time, provide a guide to the types of cybersecurity threats actors in the defense sector may encounter and should seek to protect themselves against.

The Heist: Data Theft at the U.S. Office of Personnel Management

One of the most notorious cyber attacks on sensitive U.S. government data assets targeted poorly secured information systems at the federal Office of Personnel Management (OPM). In 2015, OPM IT professionals investigating unusual network traffic discovered a breach of OPM's personnel files. Later investigation revealed attackers initially breached data networks of OPM contractors in 2013, allowing them a bridge to OPM's information systems where they systematically exfiltrated personal employee information of both federal and non-federal personnel for nearly two years. The stolen data included security clearance background information on 21.5 million current and former government employees. A Congressional committee report concluded that these attacks could likely have been prevented if standard information technology security software was up to date and if quicker remedial action had been taken during earlier security breach detections.[14] Investigators and cybersecurity analysts widely believe the attackers received backing from the Chinese government.

Data exfiltration often occurs through malware-enabled breaches. Malware can serve as a remote forward operating base for cyber attackers, independently embedding and collecting intelligence on targeted IT systems, and relaying information back to home base. Malware also can also be remotely controlled, giving attackers a back door through which they can carry out their operations. Often going undetected for long periods of time due to various masking techniques, malware allows attackers to patiently "crack" IT systems and to evade simple expulsion efforts. The OPM attackers facilitated their exfiltration by infecting OPM's networks with malware that captured the credentials of administrative-level system users, communicated information back to home servers, and enabled on-demand remote access to sensitive data.

The OPM attack demonstrates the importance of sound systems security software and processes for defending against cyber attacks. An improved defense can be as simple as requiring multi-factor authentication and vetting IT security companies who work on the software system installations. In the case of the OPM attacks, the Office of Management and Budget gave OPM guidelines for required software applications before the breach occurred and warned OPM that their systems were vulnerable to attack.

The OPM attack highlights the importance of continuous cybersecurity software maintenance and sustainment. It is imperative that leaders be aware of their cybersecurity infrastructure to direct the implementation of necessary updates and to acknowledge areas that may require improvement. Once an attack is detected, a swift reaction will limit the amount of data stolen. Additionally, evaluations should be conducted regularly to hold companies and agencies accountable for keeping software updated instead of allowing for individual discretion and, by extension, neglect.

The Flu: NotPetya's Digital Global Pandemic

Spreading globally and attacking indiscriminately, NotPetya malware exploited insecure corporate IT networks to destroy data and computer systems, serving as the tool of one of the most costly and severe cyber attacks in history. The virus initially demonstrated characteristics of ransomware, encrypting a breached system's master file and prompting the victim to pay to unlock the files. This sort of ransom note, however, was a fake. Instead, NotPetya rendered infected systems totally unusable; infected machines had to

islamic-revolutionary.; Graff, Garrett M. "DOJ Indicts 9 Iranians for Cyber Heists Against 144 Colleges." Wired. Conde Nast, March 24, 2018. https://www.wired.com/story/iran-cyberattacks-us-universities-indictment/.

12 Greenberg, Andy. "Stealthy, Destructive Malware Infects Half a Million Routers." Wired. Conde Nast, May 23, 2018. https://www.wired.com/story/vpnfilter-router-malware-outbreak/. ; Largent, William. "New VPNFilter Malware Targets at Least 500K Networking Devices Worldwide." Talos Blog || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: New VPNFilter malware targets at least 500K networking devices worldwide, January 1, 1970. https://blog.talosintelligence.com/2018/05/VPNFilter.html.

13 Goodin, Dan,"VPNFilter malware infecting 500,000 devices is worse than we thought," Ars Technica, June 6, 2018. https://arstechnica.com/information-technology/2018/06/vpnfilter-malware-infecting-50000-devices-is-worse-than-we-thought/ [Last accessed: September 26, 2019]

14 Committee on Oversight and Government Reform. "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation." United States House of Representative, September 7, 2016. http://static.politico.com/b4/98/a1b9722244ef9cb201c9ac91b668/house-oversight-gop-report-on-the-opm-data-breaches.pdf.

be replaced and, unless an off-line system backup could be installed on fresh machines, the data was irretrievable. NotPetya initially targeted a shipping firm in Ukraine that neglected to patch a well-known vulnerability in the Windows operating system. This exploit was paired with an attack on another known vulnerability in specific software used by most shipping companies. Once NotPetya found an entry point into the company's international network, its reach became global, automatically spreading the virus. From Ukraine to Pennsylvania to Tasmania, NotPetya's worldwide cyber attack inflicted more than $10 billion in damages to the global economy before it was stopped.

NotPetya serves as a classic example of an avoidable software breach. The vulnerabilities only exist when regular updates and patches are neglected—usually because cybersecurity is a low priority. Moreover, NotPetya exploited the same weaknesses as the infamous WannaCry malware several weeks earlier. NotPetya's rampage through global networks was entirely preventable as it was only made possible by gross cybersecurity negligence. Additionally, the substantial improvements NotPetya demonstrated over its recent predecessor, Petya, suggest to many experts that state-level resources were devoted to improving this latest iteration of the Petya family of malware.

NotPetya's story provides a clear warning for cyber policy leaders: supply chain cybersecurity is only as strong as its weakest link. Even large contractors with effective internal cybersecurity policies can be breached due to a subcontractor's negligent cybersecurity practices farther down the supply chain.

The Time Bomb: Collateral Damage from Stuxnet's Digital Blast for Nonproliferation

Not all historic cyber breaches immediately make themselves known. Malicious software can lurk for weeks or months after infecting a target system before taking any action. Such software can be activated by remote command, a timer, or when the host system attempts a pre-designated action. 2010's Stuxnet was one such delayed-action computer worm and stands among the earliest examples of malware designed to affect physical machinery and infrastructure.

Stuxnet is widely believed to be the product of a U.S.-Israeli partnership aimed at impeding Iran's nuclear programs by disrupting nuclear centrifuges. Spread through USB storage devices to circumvent the 'closed network' defense against cyber attacks, Stuxnet was programmed to quietly migrate from system to system until it found the proprietary Siemens supervisory control and data acquisition software configurations unique to industrial machinery like Iran's centrifuges.[15] Once ensconced within the Iranian plant systems, the worm quietly collected data on the nuclear facilities' layouts and operations for several months before carrying out its ultimate mission: the destruction of the centrifuges. To do so, Stuxnet hijacked the Siemens software controlling the centrifuges at the heart of the nuclear program and delivered instructions to induce subtle changes to the normal operation of the centrifuge turbines. These changes severely damaged critical machinery and presented the Iranian nuclear program with a significant setback.

Though designed explicitly to attack Iranian nuclear facilities, the Stuxnet worm spread to the internet at large, likely due to an Iranian nuclear site worker unwittingly carrying the worm home on a laptop. Once freed from the isolated nuclear program systems, the attack spread across the globe. Fortunately, Stuxnet was designed to activate only upon detecting the aforementioned Siemens software configuration, remaining inert on all other infected systems. Additionally, all versions of Stuxnet carried instructions to self-destruct by mid-2012. According to other evidence, these precautions against collateral damage indicate that Stuxnet was designed for an innovative surgical cyber attack on Iranian nuclear infrastructure.

While Stuxnet was designed to accomplish its specific mission and then destroy itself, it sets a concerning precedent for the use of state-designed and deployed, highly specialized computer worms that lurk in critical systems, waiting to unleash chaos when conditions are right. Such an attack could target component manufacturers and infect computer systems intended for ostensibly secure destinations, taint quality control procedures for materiel supply chains to halt production before or during a conflict, or even disrupt the continued function of the U.S. government itself. Accordingly, urgent action is required to harden supply chains as diverse and unevenly secured as that of the U.S. defense community against the threat of Stuxnet's legacy.

The Bug: Infiltrating IT Supply Chains with Electronic Surveillance

A less common but potentially devastating cyber vulnerability in the U.S. lies not in software or human error but in foreign contractor-produced hardware. Though relevant parties deny the vulnerability's existence, the Super Micro 'hack' was one of the marquee cyber breach stories of 2018. Although its factual validity remains in question, the Super Micro story can nevertheless serve to illustrate the very real threat that hardware breaches pose to U.S. infrastructure and capabilities.

A 2018 Bloomberg News report alleged that Chinese intelligence officials directed Chinese manufacturers to insert computer chips containing malicious programming into Super Micro Computer motherboards bound for U.S. telecom providers.[16] Smaller than grains of rice, these chips were designed to grant remote access to data passing through connected systems using this compromised hardware and could provide an avenue for Chinese actors to disrupt the secure operation of affected machines and processes. While Super Micro's clients firmly refuted the hardware breach allegations, the broader issue of foreign, inadequately supervised subcontractors manufacturing components for critical U.S. platforms remains a glaring vulnerability of the security of our defense supply chain network.

15 Langner, Ralph. "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve." The Langner Group, November 2013. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

16 Robertson, Jordan, and Michael Riley. "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies." Bloomberg, October 4, 2018. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

Hardware vulnerabilities present a special cybersecurity challenge. While software's malleable, updateable foundation allows patches and updates to eliminate vulnerabilities and exploits, hardware requires physical inspection and intervention to remediate affected machine components. If a component cannot be replaced or corrected, the operator must decide between allowing the vulnerability to persist or taking the affected machine offline. Taking affected components offline can have additional consequences ranging from minimal to catastrophic. For example, removing a compromised Wi-Fi chip and switching to a wired connection is much less problematic than losing functionality in a weapons platform or early-warning defensive system.

Establishing new policies to preclude such hardware exploits is much easier than addressing them after the fact. At their core, optimal conditions for foreign actors to exploit hardware vulnerabilities arise from the confluence of international supply chains and a lack of oversight. Accordingly, policies that ensure oversight and accountability within the supply chain can effectively address this source of hardware exploits.

The Dragnet: The Campaign to Capture the Navy's Sea Dragon Data

Despite only limited public reports, the hacking of a contractor working at the Naval Undersea Warfare Center (NUWC) caught NUWC off guard. Originally reported by *The Washington Post*, NUWC was hacked by actors believed to be working for the Chinese Ministry of State Security.[17] Based on the information available, it is understood that the hackers were able to exfiltrate a large amount of data relating to U.S. Navy submarine capabilities, information systems, cryptographic systems, and an anti-ship missile program known as "Sea Dragon." According to the DoD, the stolen information was unclassified but, based on certain statements, may have fallen into the category of being controlled unclassified information. The information was stored on the contractor's unclassified network.

The Chinese captured secret Sea Dragon data through a campaign that laid a trap ensnaring a large network of U.S. Navy contractors with access to project information. Accenture's iDefense unit examined the Sea Dragon hack closely by using proprietary sensor data. They found the hackers targeted not only a specific contractor but also several points on project's supply chain, including universities and government-funded research laboratories.[18] Information about the methods used can be gleaned from the attacks that occurred against educational institutions. The iDefense unit explained in its report that the hackers were likely associated with a group known as MUDCARP. MUDCARP is known to use spear-phishing to deploy malware. For the universities hacked, MUDCARP used emails designed to look like they came from partner universities. These emails had .RTF documents attached that took advantage of a Microsoft Office Exploit, allowing MUDCARP to embed malicious code within them. Additionally, they have been known to use a JavaScript backdoor and a web shell to conduct their activities. These attack vectors remain vulnerabilities across software systems used by the DoD. The full extent of the breach relating to the Sea Dragon program is unknown, but it is safe to say from the seriousness of the response level that this breach represents yet another incident in a long line of cyber intrusions.

The Poisoned Chalice: The Risk of Cyber Vulnerabilities in the Weapons Supply Chain

The sheer complexity of defense weapons systems and their supply chains creates significant cyber vulnerabilities in major weapons systems, which attackers can exploit. Although not based on a specific known attack, the U.S. Government Accountability Office (GAO) conducted a performance audit of the state of DoD's weapon systems cybersecurity between July 2017 and October 2018.[19] The report studied historic determinants of existing weapon systems cybersecurity, assessed cyber vulnerabilities in platforms currently mid-development, and reviewed DoD's cyber-resiliency plans for its weapon systems. The burgeoning reliance on software and network connectivity to enable hardware weapon capabilities "expands weapons' attack surfaces" for potential adversaries.

The GAO found DoD does not do enough to address cybersecurity in weapons system acquisitions. Evaluators discovered many DoD weapons program offices lack knowledge of the cyber vulnerabilities of their systems nor do they know how they would institute controls to reduce those vulnerabilities. GAO also found significant and preventable cyber vulnerabilities exist in many weapon systems currently under development. Some of these insecurities are based in password mismanagement, overly simplistic permission restrictions, and unencrypted communications. Evaluators took advantage of these weaknesses to gain control of different DoD weapon systems while largely undetected. The GAO notes that the lack of attention to cybersecurity in weapons system development starts at the requirement stage where regulations nor common practice emphasize cybersecurity. Traditional software vulnerability solutions like patches and upgrades may not work with software-enabled weapon systems given their complex design and geographically distributed operations. Thus, many program offices must develop system-unique cybersecurity maintenance and sustainment approaches.

The integration of software into weapons systems and the dependence on computers to control, maintain, and develop these systems has assisted the U.S. in remaining the dominant world power. However, this progression requires continued cybersecurity software maintenance and modernization to lessen the likelihood of hacks such as those highlighted in the GAO report. The DoD recognizes this fact and, to combat possible future cyber attacks, is creating and revising policies to better implement cybersecurity into weapon systems, delegating more funding to research and investigate ways to understand cyber vulnerabilities. As the military continues to move towards becoming a computer-dependent force, securing network chains is imperative for national security.

17 Nakashima, Ellen, and Paul Sonne. "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare." The Washington Post. WP Company, June 8, 2018. 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.

18 Catalan, Brandon. "Mudcarp's Focus on Submarine Technologies." iDEFENSE CYBER THREAT INTELLIGENCE BLOG. Accenture, March 5, 2019. https://www.accenture.com/us-en/blogs/blogs-mudcarps-focus.

19 Government Accountability Office. "Weapon Systems Cybersecurity DoD." GAO, October 2018. https://www.gao.gov/assets/700/694913.pdf.

THREAT MATRIX

Some cyber incidents discussed above are represented below in the format of the Cyber Kill-Chain Model of Cyber Threats as developed by the Lockheed Martin Corporation.[20] This model seeks to provide advanced visibility into attack vectors and to clearly demonstrate the evolution of a cyber attack from conception to execution.

ADVERSARY OBJECTIVE

Reconnaissance

Associated Invasive Techniques	Email harvesting; Identifying employees; collecting critical info through public documents; discovering internet-facing servers.
OPM Breach (2013-2015)	Attackers gain initial access to OPM's network and collect info on IT system architecture.
NotPetya (2017)	The attacker group named APT28, widely linked in published media to Russian military intelligence, routinely engages in vulnerability scanning and credential harvesting against target organizations.
China Telecom Internet Traffic Hijacking (2016-2017)	China Telecom began acquiring major PoPs (Points of Presence) in North American digital telecommunications networks in the early 2000s, giving it control over the flow of important nodes of internet traffic flow.
Sea Dragon (2018)	Actors from MUDCARP, a hacking group likely associated with the Chinese government, targeted the unclassified network of multiple cleared contractors at Naval Undersea Warfare Center (NUWC). They also likely targeted other DoD supply chain assets, as well as universities and government-funded research labs.

Weaponization

Associated Invasive Techniques	Obtaining "weaponized" malware vehicle: select decoy files; select backdoor implants and associated C&C infrastructure; designate specific mission ID for malware; compile the backdoor; and weaponize payload.
OPM Breach (2013-2015)	The hackers, widely believed to be backed by the Chinese government, specialize in using malware for data exfiltration.
NotPetya (2017)	NotPetya was loosely modeled on the Petya malware that featured in a major 2016 cyber attack. NotPetya integrated aspects of a leaked NSA hacking tool.
China Telecom Internet Traffic Hijacking (2016-2017)	This incident is known as a Border Gateway Protocol (BGP) hijack. In 2010, China Telecom successfully experimented with hijacking 15 percent of all internet traffic for 18 minutes.
Sea Dragon (2018)	MUDCARP is known to employ spear-phishing emails to deliver malware. MUDCARP also uses other tools such as web shells, backdoors, and brute force attacks.

Delivery

Associated Invasive Techniques	Adversary delivers malware directly against web servers; adversary delivers malware through indirect release, malicious email, malware on USB, social media interactions, and compromised websites.
OPM Breach (2013-2015)	In a second wave of attacks, attackers gained access to network of an OPM contractor. Although detected early by OPM network administrators, attackers exploited the slow and ineffective response to obtain login information for many users while engaging in a search for administrator credentials.
NotPetya (2017)	Attackers infected a popular Ukrainian accounting software platform with NotPetya. The software widely distributed the malware to Ukrainian businesses.
China Telecom Internet Traffic Hijacking (2016-2017)	As a major administrator of internet traffic, China Telecom selectively and strategically manipulated their BGP forwarding tables to misdirect traffic to come across their networks. Four instances of this activity were detected between 2016 and 2017.
Sea Dragon (2018)	For the targeted universities, MUDCARP is publicly known to have sent malicious emails disguised as emails from partner universities with the aim of acquiring information on defense projects.

20 Lockheed Martin Corp. "The Cyber Kill Chain." Lockheed Martin. Accessed September 15, 2019. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

Exploitation

Associated Invasive Techniques	Gaining network access through software, hardware, or human vulnerability; acquire or develop a zero-day exploit; adversary triggered exploits for server-based vulnerabilities and victim-triggered exploits (email attachments; malicious links)
OPM Breach (2013-2015)	Through a set of privilege escalation techniques to manipulate Microsoft's Active Directory user access control system, attackers eventually gained administrative root-level access.
NotPetya (2017)	The malware exploited a flaw in a Windows network file sharing protocol to further distribute itself to computers without the accounting software.
China Telecom Internet Traffic Hijacking (2016-2017)	Attacks involved falsely claiming ownership of destination IP addresses and/or falsifying BGP forwarding tables to indicate short routing distances between hijacker-controlled servers and destination IP addresses.
Sea Dragon (2018)	MUDCARP is known to exploit vulnerabilities in Microsoft Office. MUDCARP has used MSOS vulnerabilities to embed malicious code into .RTF documents.

Installation

Associated Invasive Techniques	Install web shell on web server; install backdoor/implant on client victim; create point of persistence by adding services, AutoRun keys, etc.; implement a "time stamp" of the file to make malware appear to be natural part of OS install.
OPM Breach (2013-2015)	Attackers installed variants of PlugX and Sakula malware to establish an open backdoor to OPM's network, aiding network navigation and data exfiltration.
NotPetya (2017)	NotPetya installed Mimi Katz tool to locate network administrator credentials in the memory of infected machines.
China Telecom Internet Traffic Hijacking (2016-2017)	In one attack that lasted six months in 2016, China Telecom rerouted traffic captured at its Toronto IP node and destined for Korea. In another 2016 example, China Telecom captured and rerouted US bank-related network traffic originating in Houston and destined for an Italian end-point by sending it through its Los Angeles IP node.
Sea Dragon (2018)	MUDCARP is also known to use a backdoor written in JavaScript, employ a web shell that allows an adversary to download files, and access the targets' Active Directory, and to determine passwords with brute force attacks.

Command and Control

Associated Invasive Techniques	Open two-way communications channel to C2 infrastructure via web, DNS, or email through an adversary or victim-owned network.
OPM Breach (2013-2015)	A malicious DLL installed on OPM's network communicates critical system information to attackers' command and control servers located at opm-security.org.
NotPetya (2017)	NotPetya installed tools on remote machines connected to infected computers to execute malicious commands.
China Telecom Internet Traffic Hijacking (2016-2017)	In the Toronto PoP attack, instead of sending traffic directly to Korea, traffic was detoured through China Telecom PoPs in North American and China before conveyance to Korea. In the U.S. bank attack, China Telecom sent the traffic to China and never redirected to the original endpoint in Italy.
Sea Dragon (2018)	MUDCARP was able to employ a JavaScript backdoor entitled "Orz" to retrieve attacker commands from compromised websites. MUDCARP created profiles on legitimate networking sites.

Actions on Objectives

Associated Invasive Techniques	Collect user credentials; privilege escalation; internal reconnaissance; lateral movement through environment; collect and exfiltrate data; destroy systems; overwrite or corrupt data; surreptitiously modify data.
OPM Breach (2013-2015)	Over a series of raids, attackers exfiltrated background investigation data for millions of personnel records.
NotPetya (2017)	NotPetya aggressively encrypted system files, including master boot records, rendering computers inoperable; it also displayed a (fake) Bitcoin ransom request on the screens of its victims.
China Telecom Internet Traffic Hijacking (2016-2017)	China Telecom analyzed siphoned data for valuable intelligence, or it changed and corrupted data to achieve tactical objectives.
Sea Dragon (2018)	During the NUWC hack, MUDCARP was able to gain access to a cleared contractor's credentials. MUDCARP was reported to have been able to exfiltrate data from an unclassified network that, when assembled, formed information of a classified nature.

SECTION II: POLICY RESPONSE TO CYBER RISK

As cyber threats proliferate across the defense supply chain, policymakers in both Congress and the Department of Defense have scrambled to implement tangible security solutions. Whole-of-government solutions have been slow to materialize, resulting in rhetoric about cybersecurity reform exceeding substance. Federal agencies have issued new statements of cybersecurity strategy and policy at a rapid pace, trying to fill the void. Incrementally, the new strategies and policies and strategies are forming a new regulatory framework for securing sensitive information, networks, and assets. A contractor attempting to navigate these documents and the current status of cyber regulations can easily get lost in the nuance and overlap. From departmental guidance to government-wide strategy documents, the following examines how spurious attempts to solve cybersecurity issues have undergone significant evolution but continue to leave new entrants and established actors in the dark about how best to combat the noted cyber threat.

NATIONAL DEFENSE STRATEGY

The 2018 National Defense Strategy forms the foundation of the emerging cybersecurity regulatory framework. It argues that the DoD must ensure that the military can fight and win in any domain, including cyberspace. The Department seeks to preempt, defeat, and deter malicious cyber activity targeting U.S. critical infrastructure, regardless of whether the potential incident could impact readiness or warfighting capability. Furthermore, it stipulates that the Department will work to strengthen cyber capacity, expand combined cyberspace operations, and increase bi-directional information sharing.

The strategy establishes five cyberspace objectives for the DoD:

1. Ensuring the Joint Force can achieve its missions in a contested cyberspace environment;
1. Strengthening the Joint Force by conducting cyberspace operations that enhance U.S. military advantages;
2. Defending U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause significant cyber incidents;
3. Securing DoD information and systems against malicious cyber activity, including DoD information on non-DoD-owned networks; and
4. Expanding DoD cyber cooperation with interagency, industry, and international partners.

To achieve these objectives, the DoD makes several commitments. It will prepare to defend non-DoD-owned Defense Critical Infrastructure (DCI) and Defense Industrial Base (DIB) networks and systems. As the Sector-Specific Agency partners with DCI and DIB, the Department will set and enforce cybersecurity standards and reporting. It will also be prepared to, when requested and authorized, provide direct assistance before, during, and after an incident.

The Department is looking at a five-prong strategic approach to achieving its objectives and meeting its commitments. The approach includes: fostering agility, automation, and data science to accelerate cyber capabilities development; conducting real-time efforts to prevent, deter, combat, and recover from malicious cyber activities; amplifying cyber capabilities by stretching alliances and attracting new international partnerships within the cyberspace; and, reforming DoD to encourage an institutional culture of cybersecurity accountability and awareness.

Last, the National Defense Strategy emphasizes the need for the DoD to cultivate talent. Not only must cyber readiness of existing forces be sustained, but the Nation's cyber talent pool must be expanded.

U.S. NATIONAL CYBER STRATEGY

The emphasis placed on cybersecurity within the National Defense Strategy spotlights the need for an updated national strategy on cybersecurity. Under President Trump's direction, the White House released a comprehensive strategy to this effect in late 2018. The National Cyber Strategy of the United States intends to demonstrate the commitment to and focus on this issue of cybersecurity at the

highest levels of government.[21] The strategy is broken into four pillars of execution.

The first pillar has a focus on protecting the American way of life by safeguarding the current systems and functions that allow for the execution of daily life. Securing federal networks and information, critical infrastructure, and combatting cyber crimes are all the subject of this pillar. This recommendation includes directing agencies to require contractors to increase their cyber protections and to ensure security measures are adopted throughout their supply chains.

The second pillar concentrates on the promotion of American prosperity through security. As the digital economy's share of the overall economy grows, so does the importance of securing this sector. Ideas are put forward in this section to foster the growth of the digital economy while ensuring security. Protecting intellectual property developed in America and developing a superior cyber workforce are also tenants of this pillar.

The remaining two pillars focus on both America's role in the world and the part that cybersecurity plays in ensuring overall peace and property. The third pillar looks at ways for the U.S. to deter future attacks by state and non-state actors through strength and dominance in cyberspace. The final pillar looks to combat would-be cyber wrongdoers by spreading America's view of internet openness around the world. Promoting open, interoperable, reliable, and secure internet across the globe to build an international community of like-minded governments and citizens is presented as another avenue to curtail the onslaught of cyber attacks.

DEPARTMENT OF DEFENSE 2018 CYBER STRATEGY

Late 2018 brought an update to the Department of Defense's Cyber Strategy document. Citing increased tensions with foreign actors such as Russia and China, this document seeks to outline the strategy needed to maintain U.S. cyberspace superiority and to stop cyber attacks before they hit U.S. networks. In this document, the Department outlines five cyberspace objectives:

1. Ensuring the Joint Force can achieve its missions in a contested cyberspace environment;
2. Strengthening the Joint Force by conducting cyberspace operations that enhance U.S. military advantages;
3. Defending U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident;
4. Securing DoD information and systems against malicious cyber activity, including DoD information on non-DoD-owned networks; and
5. Expanding DoD cyber cooperation with interagency, industry, and international partners.

Although the unclassified version of this document is light on specifics, it outlines five keys to the DoD's success in achieving its objectives:

1. Build a more lethal force.
2. Compete and deter in cyberspace.
3. Strengthen alliances and attract new partnerships.
4. Reform the Department.
5. Cultivate talent.

Each of these areas is meant to provide a roadmap for achieving the strategy's cyberspace objectives. These themes are echoed across a number of other cyber-policy documents and have influence down to the execution level at DoD.

DELIVER UNCOMPROMISED

The MITRE Corporation's Deliver Uncompromised strategy signals a response to rising incidences of data theft and other cyber breaches within the defense supply chain, and a shift in the philosophy underpinning the defense acquisitions process. It asserts that, while the Department and the broader intelligence community (IC) were "aware of cyber and supply chain threats," the U.S. lacked a unified appreciation and counterstrategy to protect these supply chains. To correct this perceived error, the strategy identifies products and services supporting national defense as potential targets for adversaries of the United States. In doing so, it placed a new emphasis on the defense community's responsibility to deploy its resources in defense of their own supply chains.

To support these efforts, Deliver Uncompromised proposes that DoD use its regulatory authority and purchasing power to establish security alongside cost, schedule, and performance as a variable in the competitive acquisitions process. Thus, the strategy suggests a new contracting status quo in which vendors and companies pursuing defense-related contracts proactively protect their extended supply networks.

As Deliver Uncompromised constitutes a policy recommendation from MITRE, a nonprofit specializing in federal research centers, the document carries no official authority in the policymaking sphere. However, MITRE wields a significant amount of influence as a thought leader in the defense community. In fact, the document had a noticeable impact on the course of DoD policymaking.

NIST 171 & DFARS 7012

With the federal government relying heavily on external service providers, having a system in place to protect sensitive federal data held within non-federal systems is of paramount importance. Recognizing this risk in November 2010, President Obama signed Executive Order (EO) 13566, Controlled Unclassified Information.[22] This order established a government-wide Controlled Unclassified Information Program. To help organizations determine what is

21 Trump, President Donald J. "United States National Cyber Strategy." National Cyber Strategy. The White House, September 2018. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

22 Obama, President Barack. "Executive Order 13556 -- Controlled Unclassified Information." Executive Order. National Archives and Records Administration, November 4, 2010. https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information.

Controlled Unclassified Information (CUI), the government has developed an online repository of information, guidance, policy, and requirements known as the CUI Registry. Only information that requires safeguarding or dissemination controls under federal law may be designated as CUI.

Executive Order 13566 requires an emphasis on the openness, transparency, and uniformity of government-wide practices. The EO also requires the National Institute of Standards and Technology (NIST) to publish a government-wide standard of cybersecurity controls resulting in the publication of NIST 800-171, which outlines how CUI is to be treated in non-federal systems.[23] These controls then apply to industry by the government through an intermeshing of requirements codified within the Federal Acquisition Regulations (FARS) and the Defense Federal Acquisition Regulations (DFARS).

Specifically, Section 204.7304(c) of DFARS requires that government contract solicitations (with an exception for commercial off-the-shelf items) include FAR Section 252.204-7012.[24] FAR Section 252.204-7012, or "7012," sets out the requirements for contractors to provide "adequate security" on all covered information systems through the implementation of the security requirements of NIST 800-171 that are in effect at the time the Contracting Officer authorizes the solicitation.[25] The version of NIST 800-171 that is currently effective is Revision 1.

NIST 800-171 rev. 1 lays out 110 separate requirements organized into fourteen "families." Each family is comprised of basic and derived security requirements. The underlying requirements originated in two separate NIST documents. While the basic requirements originated in FIPS Publication 200, the derived requirements originated in NIST Special Publication 800-53. However, the families themselves are closely aligned with the minimum-security requirements detailed in FIPS Publication 200. Without going into the specific technical requirements, the families themselves provide a broad overview of NIST 800-171's focus. The fourteen families are as follows:

1. Access Control
2. Awareness and Training
3. Audit and Accountability
4. Configuration Management
5. Identification and Authentication
6. Incident Response
7. Maintenance
8. Media Protection
9. Personnel Security
10. Physical Protection
11. Risk Assessment
12. Security Assessment
13. System and Communications Protection
14. System and Information Integrity

FAHEY MEMO

In late 2018, Kevin Fahey, the Assistant Secretary of Defense for Acquisition, addressed the amendment to the DFARS: the addition of Clause 252.204-7012 (DFARS 7012). DFARS 7012, titled "Safeguarding Covered Defense Information and Cyber Incident Reporting," requires that contractors implement NIST 171 to protect CDI that is "processed, stored, or transmitted" via the contractor's internal unclassified information systems or networks, with a specific emphasis on the "flow down" of information to subcontractors.[26] Recent successful breaches of defense subcontractors drove a desire to bolster the adoption and enforcement of DFARS 7012 cyber controls.

Fahey provided sample Statement of Work (SOW) language for use by program offices to create a standardized mechanism for tracking and recording compliance. This sample language was to be used by program offices in conjunction with sample Contract Data Requirements Lists (CDRL) and Data Item Descriptions, provided in an earlier memo issued by DPC to assess the contractors approach to achieving adequate cybersecurity.[27]

The ultimate goal of these samples and their language is to support the development of cybersecurity measures that are designed to enhance the protections of DFARS 7012. A strong encouragement was issued to program managers, requiring that they incorporate the sample language into future contracts.

LORD MEMO

To further ensure implementation of the DFARS 7012 clause, Ellen Lord, Undersecretary for Acquisition and Sustainment, issued a memo to the Defense Contract Management Agency (DCMA) to validate DFARS 7012 compliance using its existing contract administration and oversight authority.[28] This process for inspection involves (1) reviewing contractors' procedures for marking and distribution statements on DoD CUI to check for proper flow down to Tier 1 Level Suppliers, and (2) reviewing contractors' procedures to assess Tier 1 Level Suppliers' compliance with DFARS 7012 and NIST 171. DCMA began cybersecurity audits in the summer of 2019 and is seeking to ramp up audit activity by early 2020.

23 Ross, Ron, Kelley Dempsey, Patrick Viscuso, Mark Riddle, and Gary Guissanie. "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." Computer Security Resource Center. National Institute of Standards and Technology, June 7, 2018. https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final.

24 Cornell University Law School. "48 CFR § 252.204-7012 -Solicitation Provision and Contract Clauses." Legal Information Institute. Accessed September 15, 2019. https://www.law.cornell.edu/cfr/text/48/252.204-7012.

25 Undersecretary of Defense for Acquisition and Sustainment. "Safeguarding Covered Defense Information and Cyber Incident Reporting." 252.204-7000 Disclosure of Information. DARS Council. Accessed September 15, 2019. https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm.

26 Department of Defense Office of Defense Pricing and Contracting. "Safeguarding Covered Defense Information – The Basics." Accessed September 15, 2019. Safeguarding Covered Defense Information – The Basics.

27 Department of Defense Office of Pricing and Contracting. "DPAP: Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting." Department of Defense. Accessed September 15, 2019. https://www.acq.osd.mil/dpap/pdi/cyber/guidance_for_assessing_compliance_and_enhancing_protections.html.

28 Lord, Ellen. "Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review." Department of Defense, January 21, 2019. https://www.acq.osd.mil/dpap/pdi/cyber/docs/USA000140-19 TAB A USD(AS) Signed Memo.pdf.

NIST 171B

As a follow-on to NIST's initial 800-171 rev. 1 standards, the group published 800-171b to propose a heightened security standard.[29] NIST seeks for 171b to protect non-federal infrastructure storing classified information for critical programs and high-value assets against advanced cyber threats. The draft proposes applying 32 additional controls to critical programs and high-value assets, supplementing the initial 110. Pursuant to OMB Memorandum M-19-03, an agency may designate federal information as a high-value asset if it has a high informational value, it is mission essential, or it is federal civilian enterprise essential.[30] NIST created the draft of 171B with what they call the advanced persistent threat (APT) in mind. The APT is an adversary that possesses "sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors including cyber, physical, and deception." In other words, NIST's new requirements are aimed at those who play the long game in cyber warfare, establishing footholds in targeted infrastructure to be levied in the future. To combat the APT, the draft provides a foundation grounded in three components: penetration-resistant architecture, damage-limiting operations, and designing for cyber resiliency and survivability. NIST organized the draft requirements into the 14 families outlined in NIST 800-171 but did not put new requirements within contingency planning, system and services acquisition, and planning families for reasons of scope.

The draft stresses that the new and enhanced requirements apply only to the components of non-federal systems that process, store, or transmit CUI, or that provide security protection for those components when the designated CUI is contained in a critical program or high-value asset. However, if the new requirements apply, NIST's stated examples of components suggest a broad range of technologies. NIST specifically mentions mainframes, workstations, servers, input and output devices, cyber-physical components, network components, mobile devices, operating systems, virtual machines, and applications as components.

Generally, NIST explained that the requirements focus on nine key elements essential to addressing advanced persistent threats:

1. Applying a threat-centric approach to security requirements specification;
2. Employing alternative system and security architectures that support logical and physical isolation using system and network segmentation techniques, virtual machines, and containers;
3. Implementing dual authorization controls for the most critical or sensitive operations;
4. Limiting persistent storage to isolated enclaves or domains;
5. Implementing a comply-to-connect approach for systems and networks;
6. Extending configuration management requirements by establishing authoritative sources for addressing changes to systems and system components;
7. Periodically refreshing or upgrading organizational systems and system components to a known state or developing new systems or components;
8. Employing a security operations center with advanced analytics to support continuous monitoring and protection of organizational systems; and
9. Using deception to confuse and mislead adversaries regarding the information they use for decision making, the value and authenticity of the information they attempt to exfiltrate, or the environment in which they are operating.

CYBERSECURITY MATURITY MODEL CERTIFICATION

The Cybersecurity Maturity Model Certification (CMMC) program is the latest iteration of the defense department's efforts to centralize and simplify cybersecurity regulations. To this point, policy has been spurious, complex, and confusing. The CMMC seeks to centralize these strategies while also increasing the defense industry's level of cybersecurity. As of the publish date of this document, the CMMC remains in draft form with a stated implementation goal of mid-2020.

We know that the CMMC intends to cover all prime-level and subcontractors, and that enrolling in the CMMC will become a requirement for doing business with the department of defense in any capacity. The program consists of five certification levels, starting at basic cyber hygiene and increasing in complexity. Levels 1-3 will mostly consist of implementation of the NIST 800-171 standards discussed above. Levels 4-5 will be reserved for those contractors dealing with particularly sensitive programs and processes, and will mostly be analogous to the requirements put forward in the NIST 800-171b.

29 Ross, Ron, Victoria Pillitteri, Gary Guissanie, Ryan Wagner, Richard Graubart, and Deborah Bodeau. "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets." Computer Security Resource Center. National Institute of Standards and Technology, June 19, 2019. https://csrc.nist.gov/publications/detail/sp/800-171b/draft.

30 Mulvaney, Mick. "Memo for Heads of Executive Departments and Agencies." Executive Office of the President, December 10, 2018. https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf.

SECTION III: SURVEY ANALYSIS

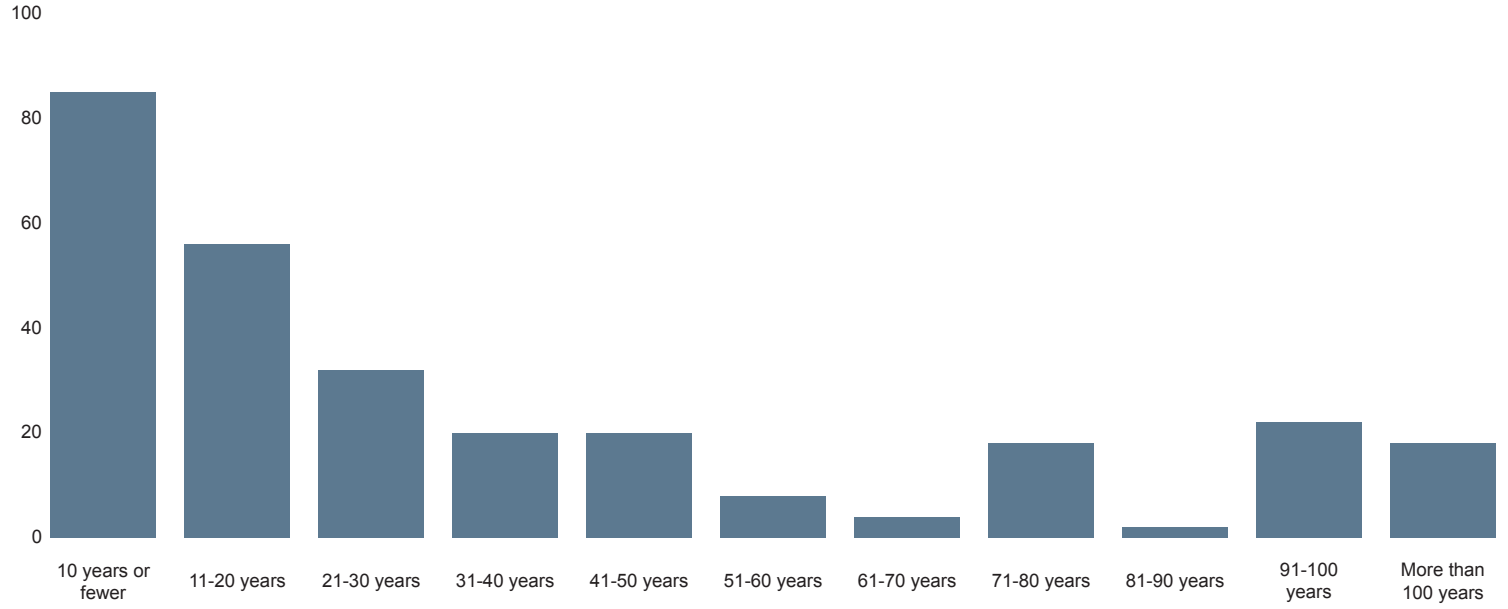
METHODOLOGY

In order to achieve a better understanding of industry behavior and attitudes toward the current cybersecurity policy environment, a working group made up of NDIA corporate staff and members of the NDIA San Diego Chapter jointly developed and administered an online survey. From April to June of 2019, a hyperlink to the survey was distributed via targeted emails to NDIA Chapters, Divisions, and individual members. In addition, the survey was highlighted on the front page of the NDIA.org website. Respondents were asked about their NDIA membership to enable the filtering of results.

RESPONDENTS' DEMOGRAPHICS

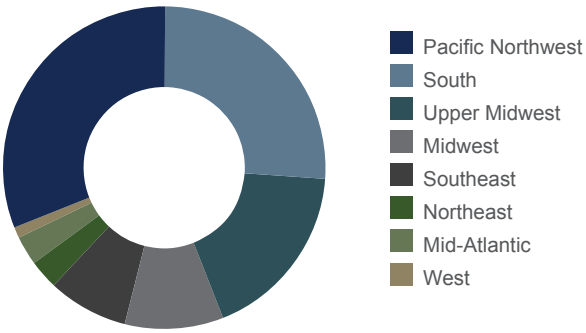
Survey respondents came from a diverse array of companies. Nearly 30 percent of all respondents work for companies launched within the last 10 years, and approximately half of them work for companies 20 years or younger in age. Comparatively, just over 21 percent of respondents held employment at companies whose origins predate the Eisenhower presidency. Respondents represent both new entrants and old veteran companies of the defense sector.

FIGURE 2: DISTRIBUTION OF RESPONDENTS BY AGE OF CORPORATE EMPLOYER



Respondents represent companies headquartered in every region of the country, with notable geographic concentrations in the Mid-Atlantic, West, and Northeast regions. These concentrations reflect concentrations of DoD expenditures and employment.[31] The small representation among respondents of firms based in the South and in the Pacific Northwest may introduce some nonresponse bias into the results and represent areas where NDIA's reach is limited. These areas should be a focus of engagement for both NDIA and the Department of Defense.

FIGURE 3: LOCATION DISTRIBUTION

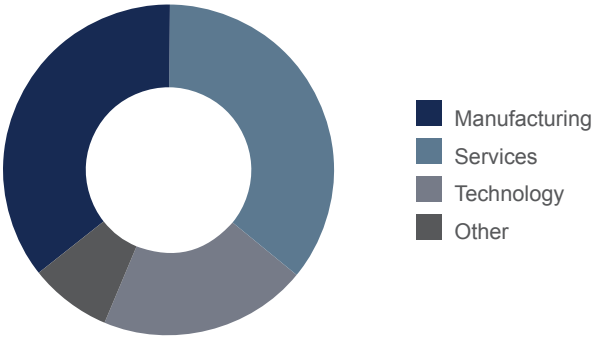


Most respondents represent for-profit defense contracting companies. Nearly 70 percent of respondents worked for privately held for-profit companies while only 23.5 percent represented publicly traded for-profit defense sector firms. Non-profit organizations, such as research institutions, employed almost seven percent, and less than one percent belonged to universities. This breakdown is approximately equivalent to NDIA's membership.

Respondents reflect a variety of industrial sectors. Asked to assign their company's government contracting work to an industrial category, 36 percent of respondents identify their employer within the "technology" sector, 36 percent chose "services," 20 percent place their company within the "manufacturing" industry, and eight percent answered "other."

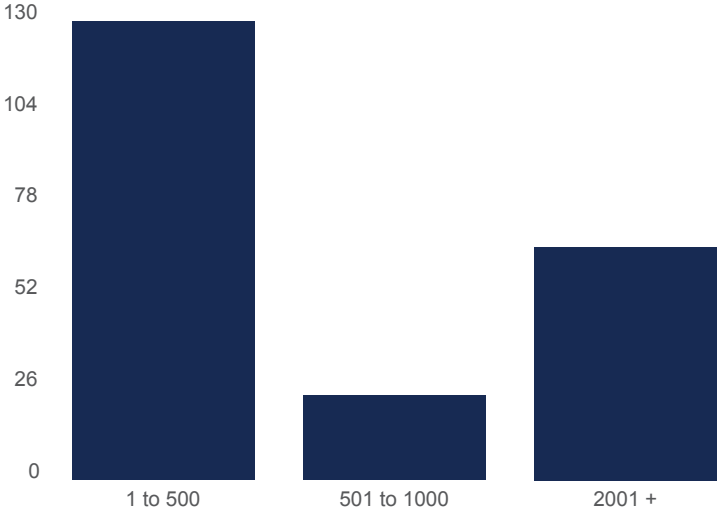
31 National Defense Industrial Association. "New Report on Defense Spending Shows Where Contracting Dollars Flow." NDIA Policy Blog, May 24, 2019. https://www.ndia.org/policy/recent-posts/2019/5/24/new-report-on-defense-spending-shows-where-contracting-dollars-flow.

FIGURE 4: PRIMARY INDUSTRY



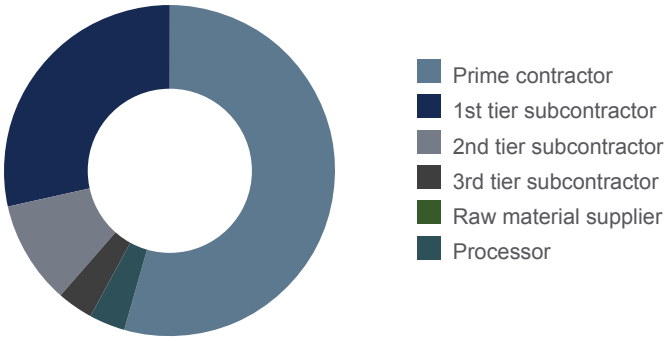
The survey drew heavy participation from both small businesses and employees of large defense contractors. 59 percent of respondents represented firms with 500 or fewer employees, while 30 percent of respondents came from firms with more than 2,000 employees. Mid-size firms saw representation from 11 percent of respondents. For the purposes of this analysis, "small business" denote those companies identifying as having 500 or fewer employees and "other than small" is used to represent those companies with greater than 500 employees. This nomenclature is used in accordance with the Small Business Administration's size standards and simplified for the purposes of this study.[32]

FIGURE 5: NUMBER OF EMPLOYEES



The body of survey respondents includes all tiers of the defense supply chain. The survey asked respondents to identify their company's primary position in the supply chain according to the work predominantly performed by the company. The majority (54 percent) of respondents indicated that their company predominantly performs as a prime contractor. 28 percent of survey takers identified as first-tier subcontractors, 10 percent as second-tier suppliers, four percent as third-tier suppliers, and four percent as materials processors. No respondents identified their company as a raw material supplier.

FIGURE 6: PRIMARY POSITION IN SUPPLY CHAIN



COMPANY FINANCIALS

Key Takeaways

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

Companies in the different tiers of the DoD supply chain have varied levels of the reliance on DoD contracts among different tiers of contractors. The survey asked respondents to provide a percent breakdown of their revenue based on the origin of their business, using the options DoD, non-DoD, State and Local Government, Commercial, or Other. The accompanying figures reveal contractors to be less dependent and focused on DoD customers as one moves down the supply chain. For example, while 52 percent of prime contractors derive more than 80 percent of their revenue from DoD, only 43 percent of first-tier subcontractors, 23 percent of second-tier subcontractors, and 20 percent of third-tier subcontractors do so. Nonetheless, the survey also shows small business contractors have less diversified revenue than do than other-than-small businesses. 52 percent of small business respondents identify DoD as the source of more than 80 percent of revenue, whereas only 38 percent of other-than-small businesses draw more than 80 percent of their revenue from DoD. Figure 7 indicates how companies responded based on their position within the supply chain. For example, five percent of the prime contractors who provided a percentage for DoD contracts indicated that DoD contracts made up 0-20 percent of their revenue.

32 U.S. Small Business Administration. "Size Standards." Accessed September 15, 2019. https://www.sba.gov/federal-contracting/contracting-guide/size-standards.

FIGURE 7: DOD REVENUE BY SUPPLY CHAIN POSITION

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

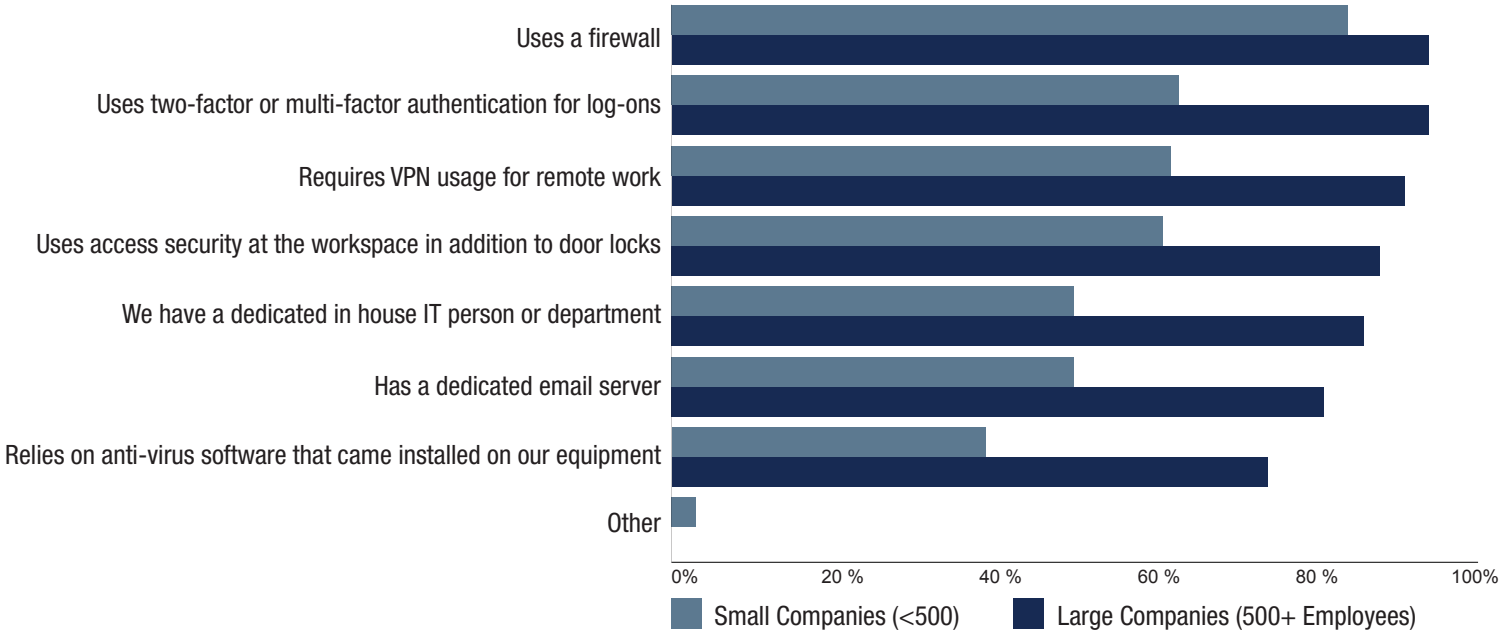
INFORMATION TECHNOLOGY

Key Takeaways

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

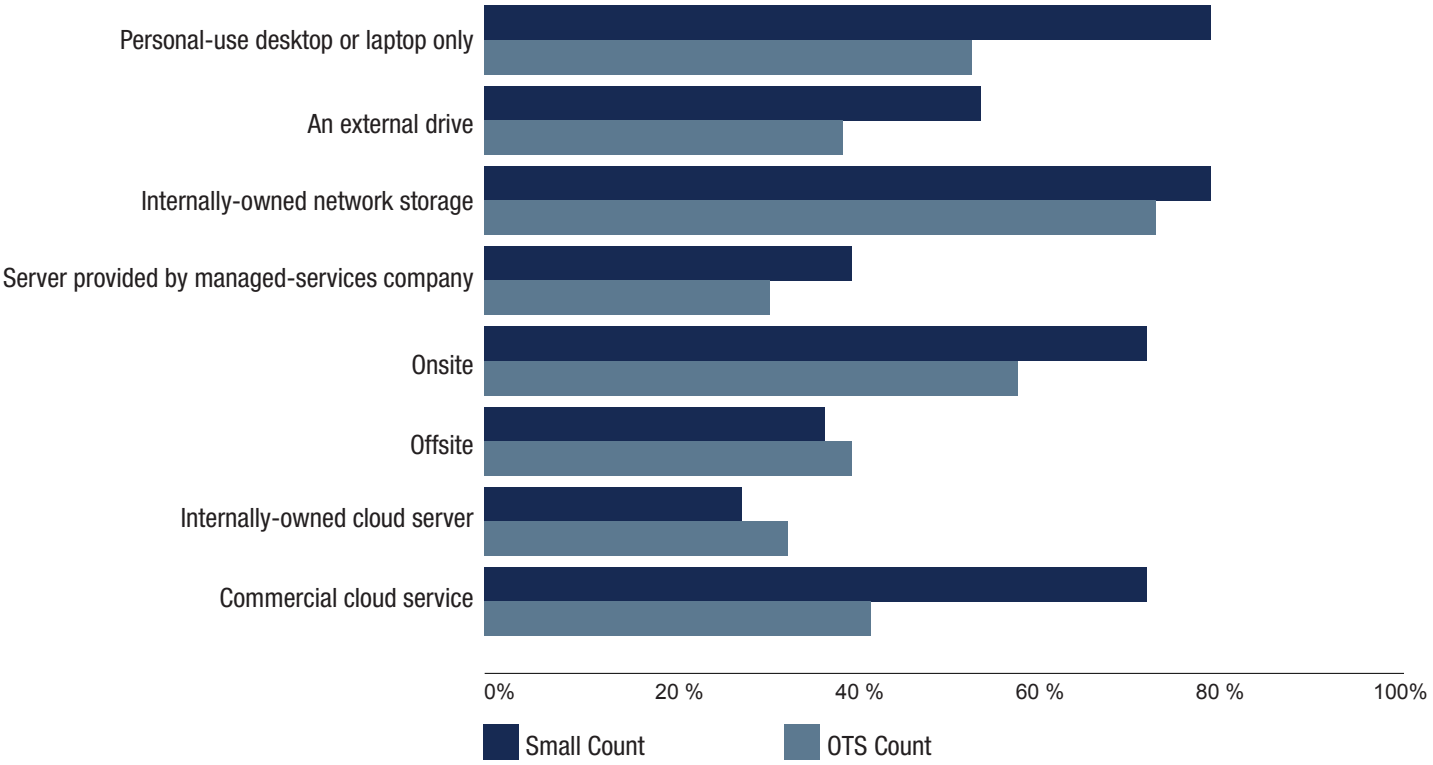
Across the defense industrial base, companies already employ a variety of measures to achieve information security goals although disparities exist among firms of different sizes. Both small (83 percent) and other-than-small (93 percent) firms widely use network firewalls to protect corporate digital information and communications. As shown in the graph below, substantial disparities between other-than-small and small firms in the adoption of more advanced security measures. For example, whereas 94 percent of respondents employed at other-than-small firms use two-factor authentication for network log-ons by employees, only 62 percent of respondents working for small firms have such a network access requirement. Similarly, while 91 percent of other-than-small contractor respondents reported being required to use VPNs for remote access to corporate network resources, only 62 percent of small firm respondents faced such a requirement. Some disparities in corporate information security measures may result from fiscal resource differences. The greater reliance on dedicated email servers and in-house IT staff by other-than-small businesses suggests that larger firms may be able to afford customized, staff-intensive information security solutions. Small firms' greater reliance on outsourced or ad hoc internal information security solutions compared with their larger counterparts supports the notion that fiscal means matter for security.

FIGURE 8: USE OF SECURITY MEASURES



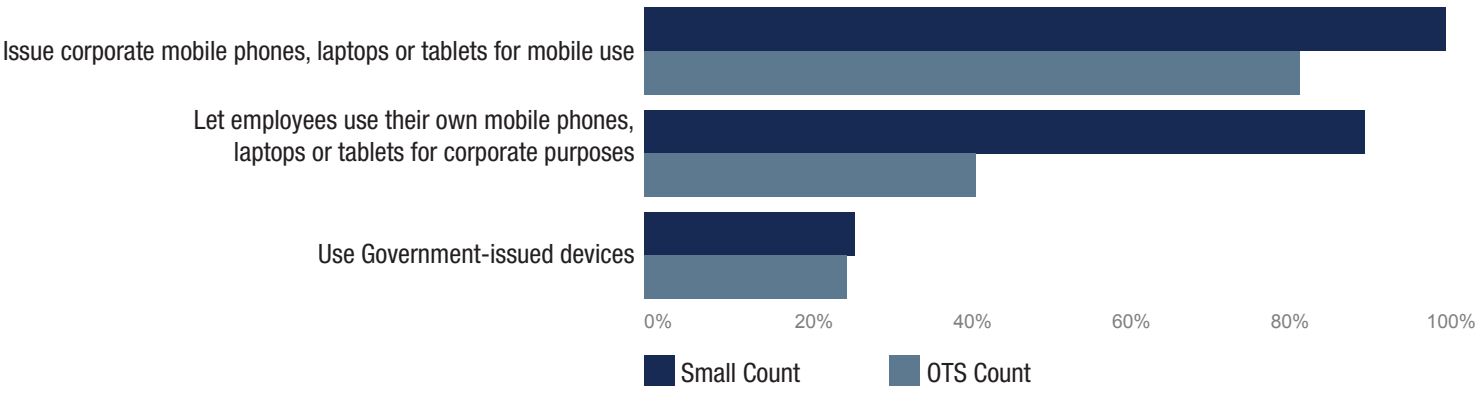
Defense contractors also vary by firm size in their handling of documents and electronic data. A majority of all respondents reported internal corporate networks (70 percent), personal-use desktops and laptops (61 percent), physical on-site archives (60 percent), and commercial cloud services (53 percent) as permitted storage methods for business-related data and documents. Large firms proved to be more selective than small firms in authorizing data storage methods. Only internal network storage and physical off-site storage received recognition from a majority of large respondents as authorized data storage methods. A majority of small firms reported personal-use computers, external drives, internally owned networks, externally managed servers, physical on-site archives, and commercial cloud services as permissible options for storing data and documents.

FIGURE 9: DATA STORAGE METHODS



Beyond permitting multiple methods for data access and storage of various security levels, companies across the defense industrial base commonly issue and/or allow use of mobile personal electronics for use in accessing corporate information technology networks. When asked to identify whether their company issues devices or if employees are permitted to use personal devices, just over 82 percent of respondents said their companies issue corporate devices. Almost 60 percent responded that their company allows allow personal device use within the company's networking environment. As shown in Figure 10, small firms tend to have more permissive policies for mobile productivity devices. Most small firms allow for the use of company-issued, government-issued, or privately owned devices. By comparison, for each of these categories, less than half of other-than-small contractors permit usage.

FIGURE 10: DEVICE USE POLICY



COST ESTIMATING AND ACCOUNTING

Key Takeaways

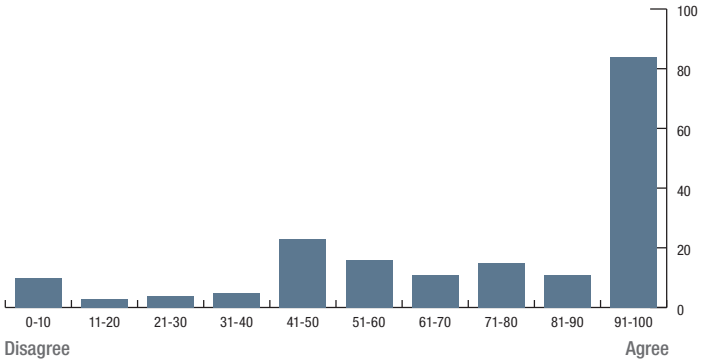
- *The majority of respondents view security-related costs as a cost-driver when pricing contract bids*
- *Industry supports treating costs associated with carrying out DFARS 7012 requirements as direct costs*
- *Nearly half of respondents have not estimated the cost of DFARS 7012 compliance*

Contractors are unified in their beliefs about how the costs of cybersecurity regulatory compliance should be handled. Before the awarding of a contract, the Defense Contract Audit Agency evaluates the cost accounting system and practices of prospective awardees for compliance with criteria established in the DFARS and specified on form SF 1408. Although nearly 70 percent of survey participants use a cost accounting system approved by DCAA, contractors with more than 1,000 employees use compliant accounting systems at more than twice the rate of companies with 20 or fewer employees.

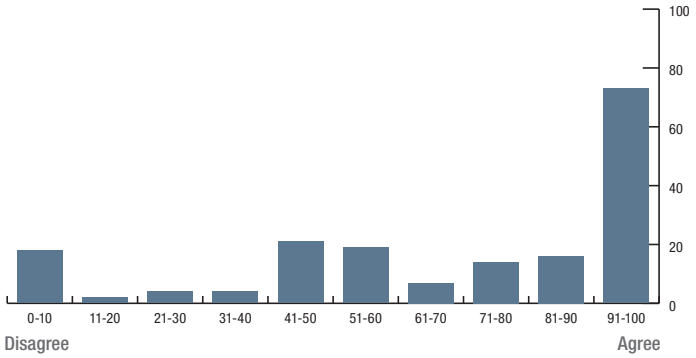
Most participants confirmed that they view security-related costs, in general, as a factor in their contract pricing proposals. Contractors also confirmed treating the DFARS 7012 cybersecurity requirements as "overhead" to be integrated into pricing estimates for DoD contracts. Contractors also are supportive of the idea of treating DFARS 7012 compliance expenses as direct costs for the contract rather than indirect costs. Whereas contractors can recoup direct costs by assigning charges to the bottom-line cost objective of the contract, indirect costs must be associated with intermediate cost objects.

FIGURE 11:

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

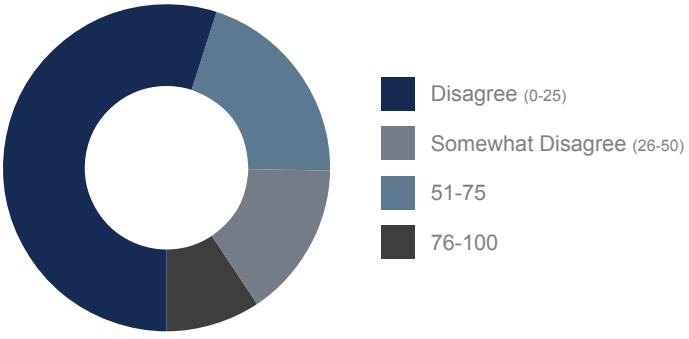


"We view DFARS 7012 costs as part of our corporate overhead that we factor into our DoD pricing."



Although most contractors believe DFARS 7012 compliance costs should be directly allocable, many contractors have yet to estimate their own costs of achieving DFARS 7012 compliance. Almost as many contractors have not completed such an estimate (40 percent) as have done so (44 percent). Nonetheless, nearly 75 percent of contractors believe their efforts to comply with DFARS 7012 will be a major cost-driver for their company's operations. One consequence of this discrepancy is that some contractors may be making decisions about DFARS 7012 compliance based more on fearful anticipation of costs rather than empirical estimates of their particular business operations and circumstances.

FIGURE 12: AGREEMENT WITH THE STATEMENT "WE SHOULD BE ABLE TO DIRECTLY CHARGE DOD FOR THE COSTS OF COMPLYING WITH DFARS 7012"



CORPORATE OPINIONS

Key Takeaways

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

Today's defense industry faces a myriad of cyber-related threats. From foreign actors to insider threats, firms must fortify their cyber defenses against a range of actors or suffer attacks like those described in this report. While it is difficult to objectively state which cyber-related threats are the most threatening to industry, it is possible to characterize which of these threats firms find most threatening from their perspective. A set of ten threat vectors were presented to survey respondents to get at this question. Listed below are the threat vectors in descending order of threat to the respondents' firm. The most threatening attacks are those from outside actors and insider threats, followed closely by a potential loss of infrastructure (power or internet outage) that would leave firms open to cyber incidents. Interestingly, we see that firms are least worried about flow-down provisions that are placed on a subcontracting firm by a prime contractor.

FIGURE 13: RANK THE BIGGEST THREATS FACING INDUSTRY

RANK	THREAT
(Most) 1	A cyberattack by an outside actor
2	A disgruntled or former employee wreaking havoc on our systems
3	Loss of infrastructure (for example, power outage, fire, or environmental event) that could degrade our cybersecurity
4	Being found responsible for a major security breach that impacts personnel
5	An audit by DoD on our cybersecurity program
6	Having contract recovery action taken against us by DoD or a prime for noncompliance
7	Being found responsible for a major security breach that impacts public safety
8	Being sued by our prime contractor for noncompliance
9	Our contracting officer doesn't understand cybersecurity at all, and will impose unrealistic audit requirements
(Least) 10	Our prime contractor is going to use these requirements to squeeze us right off the contract

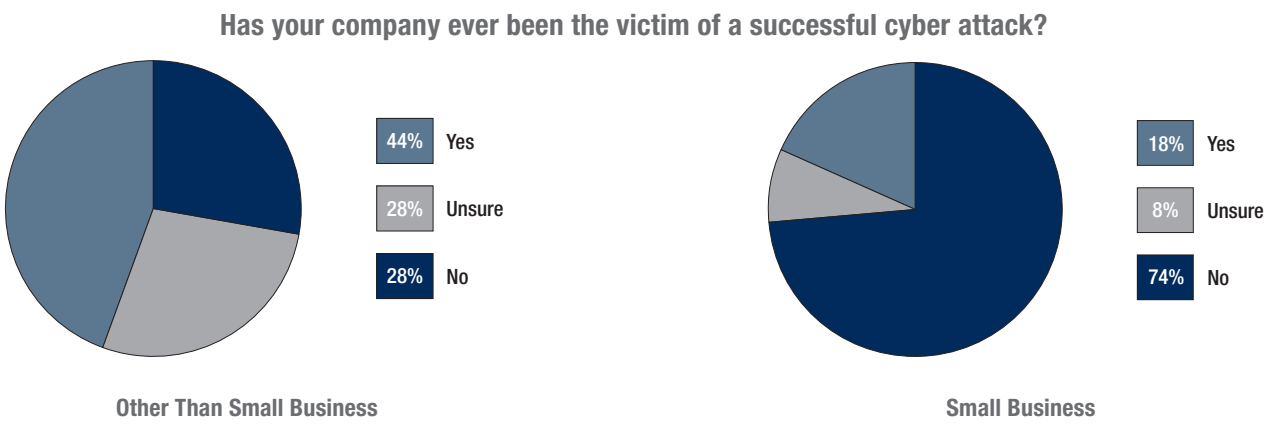
A cyber attack by an outside actor is not only viewed as the most threatening cyber attack vector but is also viewed by industry to be the most likely type. As demonstrated above, outside actor attacks can take several forms and range in severity. Industry's belief that attacks by outside actors are the most threatening and most prevalent of cyber threats should serve as a guide for policymakers seeking to fortify systems. "Having our contract rescinded by a contracting officer or a prime contractor because of poor cybersecurity implementation" was ranked as the least likely to occur, indicating that industry does not currently feel threatened that contracting officers or prime contractors will rescind their contract as a result of a cyber-related incidents. The new policies discussed above that seek to strengthen cyber standards will most likely have an impact on this perception.

FIGURE 14: RANK THE LIKELIHOOD OF EVENTS

RANK	THREAT
(Most) 1	A cyberattack by an outside actor
2	An audit by DoD on our cybersecurity program
3	A disgruntled or former employee wreaking havoc on our systems
4	Loss of infrastructure (for example, power outage, fire, or environmental event) that could degrade our cybersecurity
(Least) 5	Having our contract rescinded by a contracting officer or a prime contractor because of poor cybersecurity implementation

Given the hypothesis that cyber-related incidents are widespread throughout industry, a measure was taken of whether the participant's company had ever been the victim of a cyber attack. Many participants (42.5 percent) claimed that their company had been a victim of a cyber attack, with a sizeable group (30 percent) of participants being unsure. Those that have not experienced a cyber attack (27.5 percent) may not be in a need-to-know position within their company to be informed in the event of an attack. This data shows that it is increasingly rare for a company to go without a cyber intrusion.

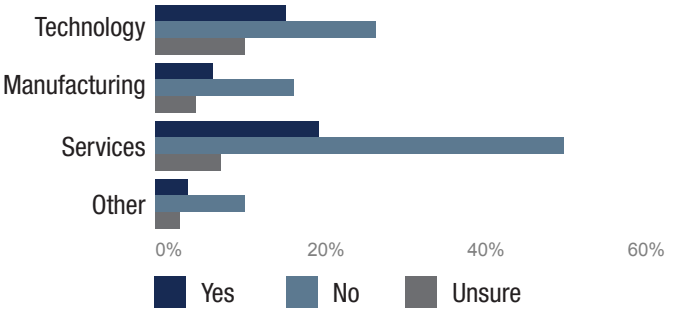
FIGURE 15: PREVALENCE OF CYBER ATTACKS



As a theme throughout industry, experiences differ between small and large companies. In the case of cyber attacks, there is a stark contrast between small and other-than-small businesses (those with more than 500 employees). Small companies were much more likely (74 percent vs. 28 percent) to answer that they had not been the victim of a cyber attack. One reason for this outcome may be that small businesses are less attractive targets to would-be hackers; another reason may be that they do not have robust enough security to detect when hacks occur.

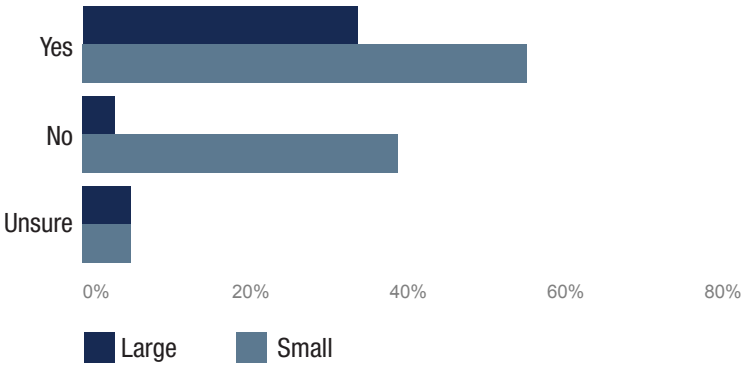
The disparity of reported cyber attacks between large and small businesses is not present when breaking out attacks by industry sector. Shown below, there is very little difference in reported cyber attacks across different sectors.

FIGURE 16: PREVALENCE OF CYBER ATTACK BY SECTOR



With such a high overall percentage of industry experiencing cyber attacks, it is prudent business planning to ensure that there is a good understanding of the costs associated with responding to and recovering from a cybersecurity incident. One bright spot from survey respondents is that a large majority (80 percent) cited that their company does have a sense of the cost associated with mitigating the after-effects of a cyber attack. Of the group that does not have a good sense, the majority falls into the small business category. Almost 40 percent of small business respondents answered that they do not have a good sense of the cost of recovering from a cyber incident. This result is especially troubling because small companies, when victim of these attacks, have fewer resources at their disposal to help bridge work stoppages, any loss of intellectual property, or temporary losses in revenue. This vulnerability should be an area of focus for the Department of Defense to help these companies not only mitigate the risk of cyber attack but also ensure that they have a good understanding of the cost of responding to these incidents.

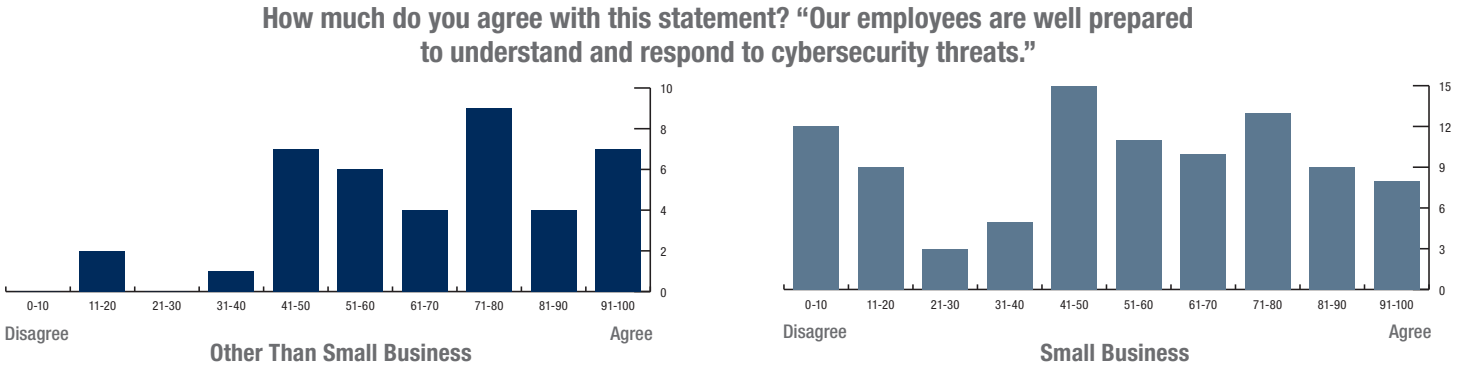
FIGURE 17: DOES YOUR COMPANY HAVE A SENSE OF THE COST FOR RESPONDING TO/RECOVERING FROM A CYBERSECURITY INCIDENT?



There will continue to be cybersecurity incidents, even in a world where universal compliance with robust cybersecurity policies exists. Quick reaction to and recovery from these incidents dramatically reduces the long-term costs associated with an attack. The first 24 hours are often a critical measure of a company's ability to mitigate damage. Industry members on average rate their confidence to recover from a cyber incident within 24 hours at 60 percent, with fairly low differences between small business (57 percent) and other-than-small businesses (68 percent). While not a perfect predictor of a company's ability to minimize the damage from a cyber incident, it is heartening that the majority of industry members feel comfortable with the 24-hour timeline. Additionally, the level of confidence displayed by small businesses is a particular bright spot for a group that is, in some metrics, behind the larger companies in robustness of cyber practices.

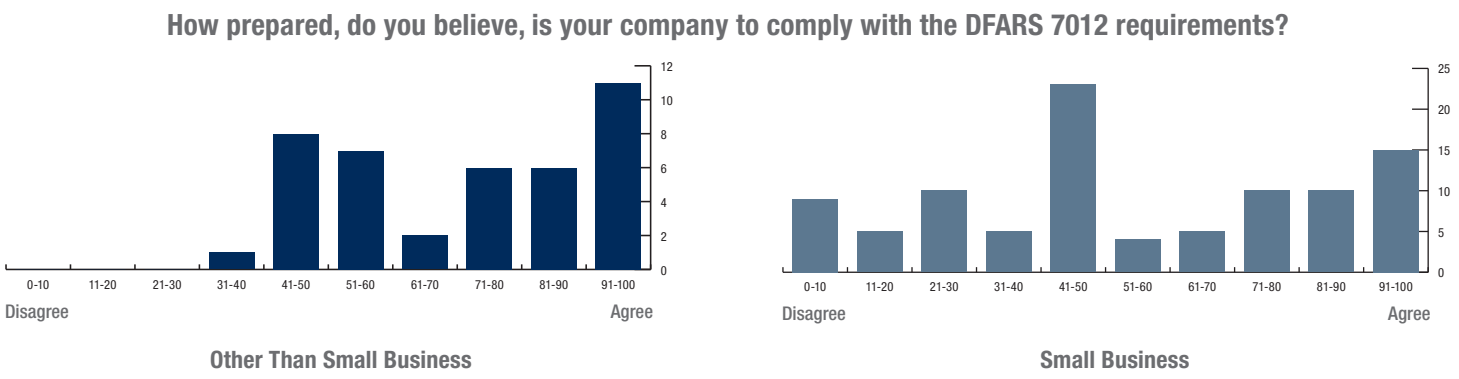
Small businesses, however, are woefully behind larger companies when rating their level of agreement with the statement "our employees are well prepared to understand and respond to cybersecurity threats." At an average agreement level of 15 percentage points lower (52 percent for smalls versus 67 percent for other-than-smalls) than larger businesses, this result marks an area where small business needs improvement. Larger companies often excel in the creation and distribution of tutorials and how-to's on avoiding and responding to cybersecurity threats. This practice should be mirrored at the small business level to close this agreement gap.

FIGURE 18: "OUR EMPLOYEES ARE WELL PREPARED TO UNDERSTAND AND RESPOND TO CYBERSECURITY THREATS"



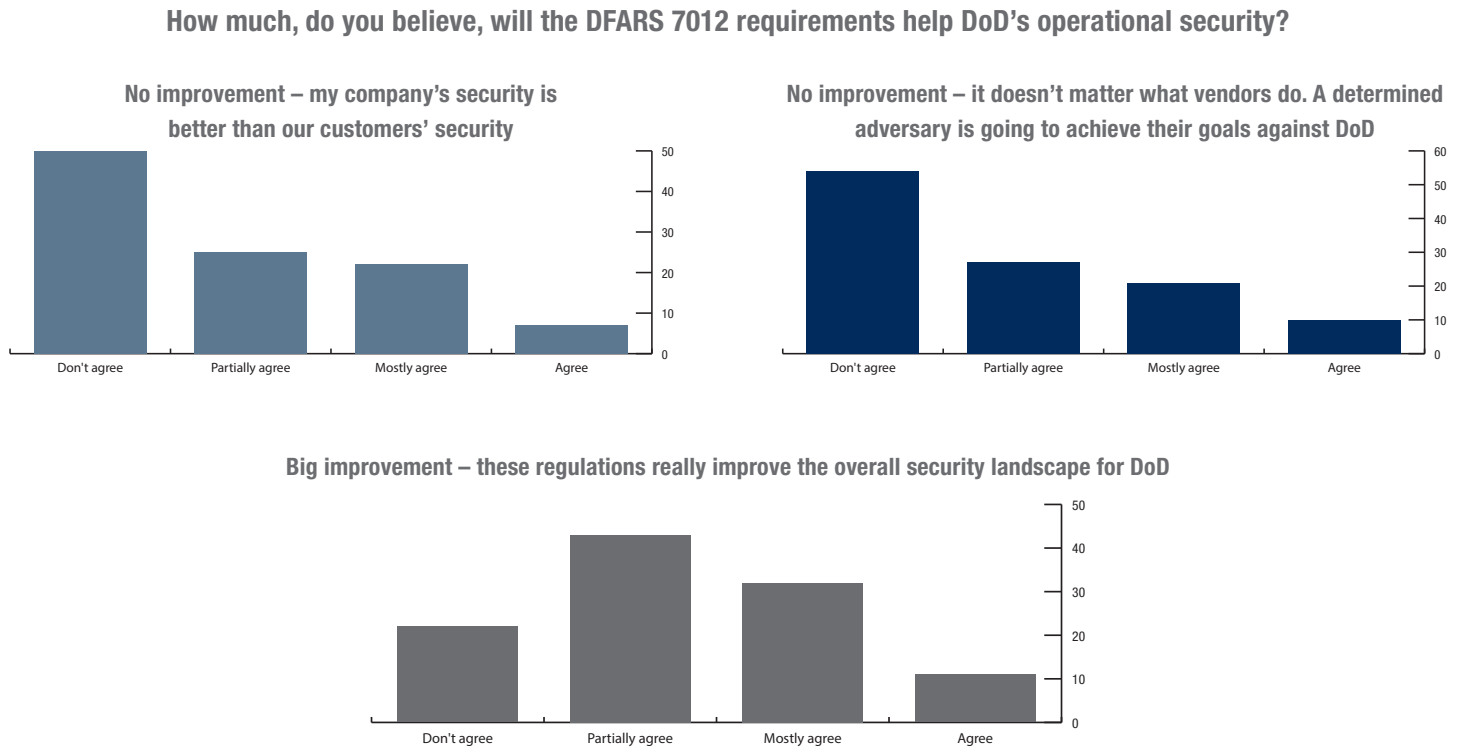
At a time when the Department of Defense is seeking to make a change to the cybersecurity requirements through the implementation of the new Cybersecurity Maturity Model Certification program, the level of adoption and compliance with the current cyber provisions included in contracts is worrisome. DFARS 7012 requirements are invoked through current contracts between the Department and prime contractors, and outline a number of cybersecurity requirements for both the prime-level and lower-tier subcontractors. While larger, other-than-small contractors have highly rated their ability to comply with DFARS 7012, we see a notable drop-off for small businesses. These businesses, which make up a large portion of the defense industrial base, rate their ability to comply with DFARS 7012 at a much lower average than larger businesses (54 percent for small vs. 72 percent for other-than-small). As the Department seeks to adopt a more exhaustive cyber standard through the CMMC program, these businesses are at risk of being woefully unprepared.

FIGURE 19: ARE YOU PREPARED TO COMPLY WITH DFARS 7012?



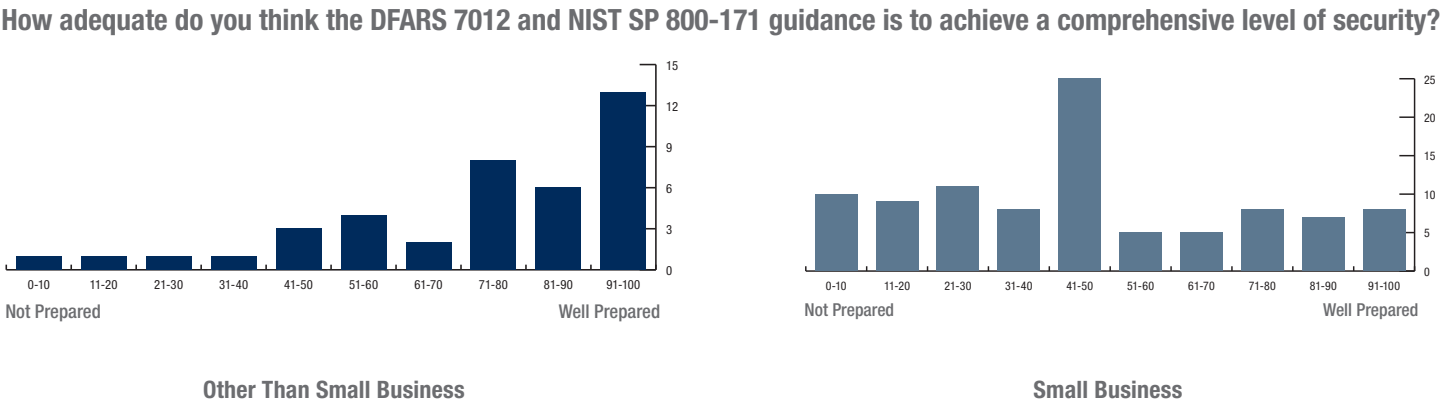
One factor potentially impacting industry's preparation for compliance with current cyber regulations is their opinion on how effective these cyber policies are in helping the government to achieve an acceptable level of security. Generally, industry members agree that implementation of DFARS 7012 policies will improve DoD's operational security. Industry also found these regulations to be a big improvement over their own security policies and felt these regulations would help to deter even the most determined adversaries from achieving their intrusion goals against DoD. While these policies may not be universally praised, it is a safe assumption that industry as a whole believes these policies will result in increased operational security for the government.

FIGURE 20: HOW MUCH WILL DFARS 7012 HELP DOD'S OPERATIONAL SECURITY?



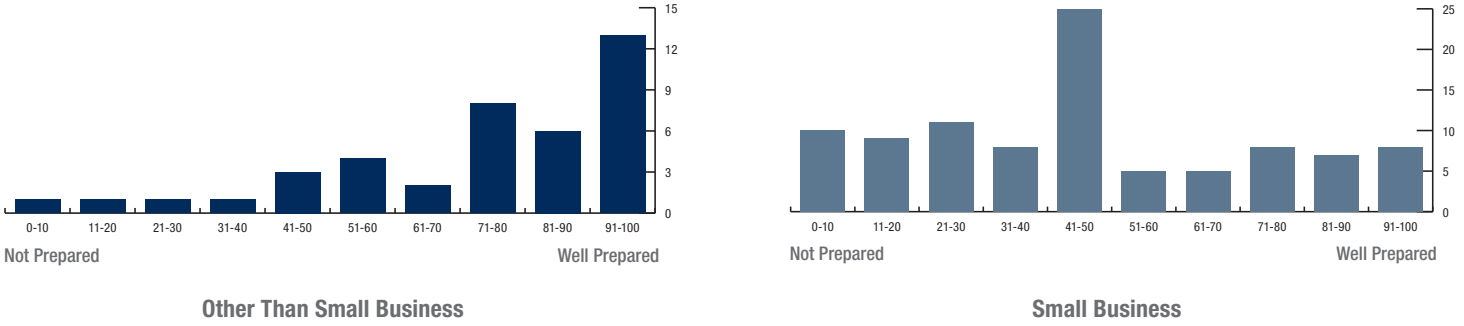
Assessments were also taken on the industry side of how impactful DFARS 7012 will be on increasing industry's cybersecurity. Across the board, there is skepticism that adherence to these two standards will "achieve a comprehensive level of security." An overall level of agreement of 56 percent is mirrored when breaking out the results for small business and other-than-small businesses. This evident skepticism of the security achieved by these two policies may be addressed by the DoD as they move towards the CMMC program, which is stated to be more comprehensive. However, it would likely serve the DoD well to seek input from industry members on how exactly to boost the comprehensiveness of cybersecurity policies.

FIGURE 21: HOW ADEQUATE IS DFARS 7012 IN HELPING YOU ACHIEVE A COMPREHENSIVE LEVEL OF SECURITY?



One piece of the current cybersecurity policy enforcement regime that is likely to continue under the next set of cyber-related requirements is the ability for the Defense Contract Management Agency (DCMA) to execute cybersecurity audits of a company. Industry as a whole rated its agreement with its level of preparedness for a DCMA audit at 56 percent. Both prime-level contractors and lower-tier subcontractors rated their level of preparedness at a similar level. As the DCMA ramps up their number of cyber audits, industry as a whole will hopefully increase this level of preparedness.

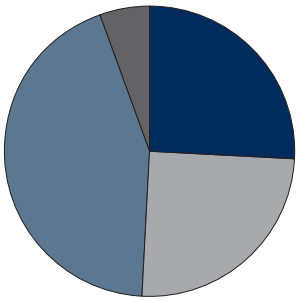
FIGURE 22: PREPAREDNESS FOR DCMA CYBER AUDIT



Digging deeper into DFARS 7012 compliance is the piece of the regulation that requires all prime contractors to flow down a requirement to their subcontractor(s) to receive and maintain a system security plan (SSP) from each subcontractor. SSPs are meant to serve as documentation that subcontractors have adequate cybersecurity controls and a mitigation strategy in place in the event of a cyber incident. Shockingly, however, 44 percent of prime contractor respondents do not have a documented SSP from their subcontractor(s). This fact documents a very serious threat within the defense supply chain. Of prime contractor respondents, only 26 percent have a documented SSP and another 25 percent have requested but not yet received an SSP. As of the date of this questionnaire, only five percent of prime contractors had taken corrective actions to reprimand their subcontractor for failing to provide an SSP. While we do commend these prime contractors for taking remedial steps, these actors only represent a small percentage of respondents that are currently in violation of cyber regulations.

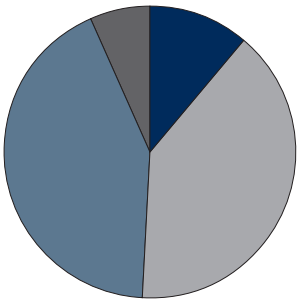
FIGURE 23: COMPLIANCE WITH DFARS 7012

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



- 5% — No, and we have taken corrective action against the subcontractor
- 44% — No, we do not currently have a documented System Security Plan (SSP) from the subcontractor
- 25% — We have requested an SSP from the subcontractor
- 26% — Yes, we have a documented SSP from the subcontractor

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



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

On the subcontractor side, a similar issue is present. Of the subcontractor respondents, 43 percent were only made aware of cyber hygiene requirements by their contract with the prime contractor. While it is heartening that 40 percent claim that the prime contractor explicitly made them aware of DFARS 7012 requirements, only 11 percent checked the stronger answer stating that their prime contractor provided information on how to comply and has been accessible for questions and discussions on the requirement. Another six percent of subcontractors claim to not handle any controlled unclassified information (CUI) and were not subject to the requirement. Although an obligation is present for prime contractors to flow down DFARS 7012 requirements, the lack of requirement to inform and educate subcontractors on the details of the requirements is apparent in the lack of familiarity with the requirements cited herein. This information disparity is most likely also contributing to the high number of SSPs not delivered by subcontractors to prime contractors. A lack of education about the DFARS 7012 requirements and other cyber policy is an apparent issue at the subcontractor level and needs to be addressed at both the government contract officer and prime contractor levels. Without this effort, it is unlikely that DoD will achieve its stated cybersecurity goals.

With the need for increased education and understanding of cybersecurity policies comes the imperative that senior business leaders within the defense contracting community prioritize the importance of cybersecurity compliance. Creating a culture of cyber hygiene and cyber regulation compliance is a necessary step in fortifying our defense industrial base against cyber intrusions. Current evidence shows that senior leaders are on the right track in prioritizing compliance. On a scale of 1 to 100, 1 being disagree and 100 being agree, respondents ranked their agreement with the statement “our senior management has communicated that [DFARS] 7012 compliance is a priority” at an average level of 64. This result indicates that most senior managers are already communicating the importance of cyber policy compliance. It is also encouraging that there was no significant difference between the answers of small versus other-than-small businesses, or prime versus subcontractors. While there is still evidence that some industry members disagreed with this statement, indicating that cybersecurity compliance has not been communicated as a priority, the majority of industry is doing its part to emphasize the importance of compliance.

A number of resources have been created and deployed in both the private and public spaces to try to increase education about cyber policies. These resources, however, are underused. Almost half of industry has not taken advantage of any outside education or training on the current DFARS 7012 requirements. This reality is potentially worrisome when paired with other data about levels of adoption and compliance. A few resources that have proven popular are trainings at industry conferences, commercial security trainings, and trainings conducted by external consultant subject-matter experts. NDIA’s own work in this area has been underutilized, with only 14 percent of industry claiming to have attended an educational session on cyber hosted by NDIA. As the regulatory landscape continues to evolve around cyber with the introduction of the CMMC program, the importance of the success of these educational tools will continue to grow. DoD should look to the areas below and tailor education efforts around the CMMC program to align with the types of programs and resources that have already been successful for industry.

FIGURE 24: USE OF CYBERSECURITY EDUCATIONAL RESOURCES

47% have not attended any outside education or training for DFARS 7012 requirements.

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

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

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

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

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

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

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

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

SECTION IV: CONCLUSIONS & RECOMMENDATIONS

It is without question that the operational cybersecurity of both industry and government must improve to meet the increased threats from foreign states and rogue actors. Visible examples of breaches at every level of the industrial supply chain and across government agencies should be enough to convince government and industry that changes need to be made. Current policies are complex while the evidence presented above shows that adoption levels are at critically low rates. The persistence of vulnerabilities will perpetuate the cycle of high-profile breaches followed by outraged responses from policymakers. Industry and government must work together to solve this issue in a mutually beneficial and expeditious manner, or risk a reactionary policy response and the continued loss of valuable data.

RECOMMENDATIONS FOR GOVERNMENT

The government should begin by increasing communication and access to resources available to lower-tier, smaller members of the defense industrial base. A disparity in resources and adoption between large and small businesses is present throughout the survey results discussed above. Data shows that smaller companies are less fortified against cyber attacks and less prepared to respond to them once they happen. These pieces work together to compound the negative impacts of cyber attacks, leaving small businesses offline for longer while threatening their ability to remain a going concern. Free and subsidized cyber resources should be made available and advertised to small businesses to aid in their knowledge about cyber hygiene and to help them prepare for inevitable attacks.

The government should also do what it can to make businesses less attractive targets for cyber attackers. The current system of turning over troves of valuable technical data to industry places an undue burden of responsibility on industry partners and makes them a target. Oftentimes, industry members receive technical or other information that is extraneous to the contract they hold. Government should work to “right-size” the amount of information turned over to industry, giving contractors only what is necessary to deliver their product or service.

Compliance with and an understanding of current rules and regulations must be better communicated to industry by government. Currently, industry is forced to interpret various contract provisions, memorandums, and armed service-specific policies to determine the cyber requirements applicable to their work with the government. This workflow increases costs for all parties and creates unnecessary barriers to entry for industry. Small or nontraditional defense contractors are particularly discouraged by the complexity of the current cybersecurity regulatory state. New policies should be all-encompassing, simple, and clearly communicated to industry to be effective and ensure widespread adoption.

The Department of Defense’s move toward the Cybersecurity Maturity Model Certification shows promise in improving the status quo of cybersecurity regulations. DoD representatives tasked with developing the program have already made considerable efforts to engage industry. These efforts should continue as the draft CMMC policies are developed. Additionally, recommendations from industry should be taken seriously. As with the current state of DFARS 7012 regulations, this new program has a risk of being too complex or burdensome, preventing widespread adoption and leading to the perpetuation of cyber vulnerabilities. Costs associated with CMMC compliance should be accurately estimated and communicated to industry partners as soon as possible to ensure that companies of all sizes can prepare to expeditiously comply.

Maintaining a healthy, robust, and secure defense industrial base is vital to the continued success of the warfighter. The Department of Defense and government as a whole must do what is possible to simplify and strengthen current cybersecurity regulations while working with industry to increase adoption and facilitate compliance.

RECOMMENDATIONS FOR INDUSTRY

Government alone is not able to solve the issue of cybersecurity. The defense industrial base has established itself as a vital partner to continued U.S. military success and must be an equal partner in fortifying itself against cyber threats. Prime actors all the way down to the single-employee subcontractors must take the threat of cyber breaches seriously and work together to keep valuable defense-related information out of the hands of those wishing harm against the United States.

Prime-level contractors should use their leverage on the supply chain to amplify government communications about the risk and rewards of cybersecurity. Primes often have direct experience with responding to and thwarting cybersecurity threats including best practices and helpful resources. This information should be shared with lower-tier supply chain members. This exchange will help to fortify smaller businesses by familiarizing them with known cyber risks.

Large businesses should also work with government on right-sizing the amount of information being flowed down through the supply chain. Minimizing the amount of data transmitted from government to a prime contractor should be mirrored when flowing information between prime and subcontractors. Making both prime and subcontractors less attractive targets will help industry as a whole decrease the number of successful breaches.

Industry must engage with government as the CMMC program continues to develop. The development of this new policy presents a unique opportunity for industry to work with government to share both its past experiences and where it sees potential for improvements to the current system. This new policy has the potential to be a panacea for industry and government by improving operational cybersecurity—but not without substantive input and from engagement by industry experts.