White Paper on the Cost of the Cybersecurity Maturity Model Certification

By: Katie Arrington, former Department of Defense Chief Information Security Officer for Acquisition and Sustainment and CEO of LD Innovations

Cybersecurity of the Defense Industrial Base (DIB) has been an imperative since 2013 when former President Obama executed the EO 13636 and then updated in 2015. Then former President Trump following up with EO 13800 and now Pres Biden with EO 14028. This has been an issue that is bi-partisan and will continue to be the weakest link in our national security until we as a government realize the cost of securing our country.

Why has this been a main concern for the past 12 plus years? Cybercrime now costs the world almost $600 billion, or **0.8 percent of global GDP**, according to a new report by the Center for Strategic and International Studies (CSIS) and McAfee.

The National Institute of Standards and Technology (NIST) have and will continue to create and update many different standards to best protect networks, software, etc. As we are well aware that we are in a state of electronic warfare and the tactics, tools and methods are always changing, so their job will never be done. We have an International Standard Organization (ISO) who as well has the (ISO) 27001 that many of our international partners use for cybersecurity standards and compliance. The challenge for the Defense Federal Acquisition Rule (DFAR) 252.204.7012 Safeguarding Covered Defense Information and Cyber Incident Reporting which required contractors to implement the NIST SP 800-171 "Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations" sadly, when this was put into effect in 2015, there was not a requirement for the government to do an analysis of costs to industry and it allowed contractors to self-attest to their compliance with the requirements. This is where the entire effort got off track and our adversaries have been exploiting this for years.

What that means is that the DIB was not taking security as seriously as government wanted and although there has been legislation in the NDAA and EO's, the funding has never been appropriated for the additional requirements set forth in 2015.

There has been an independent 3rd party study conducted (focused on small business DoD Primes and Subs) to provide a better understanding/profile of where the DIB is in their seriousness of implementing CMMC requirements. The institution did both a preliminary qualitative research phase to provide a depth of understanding and the foundation for a subsequent quantitative phase which followed phase one. This I am sure will be released in the coming days or week.

But in the meantime, during this month’s town hall, DIBCAC Director for the Defense Contract Management Agency (DCMA), Nick DelRosso joined the Cyber AB as a staff to provide insights into the results and trends which have been encountered during DIBCAC assessments of DIB organizations. Here are some of the key takeaways from his presentation:

- DIBCAC has curated a list of the top 10 NIST 800-171 requirements that were determined to be other than satisfied “OTS”. These controls (listed in order of frequency) included: FIPS Validated Encryption (3.13.11), Multi-factor Authentication (3.5.3), identifying, reporting, and correcting system flaws (3.14.1), Periodically assessing risk (3.11.1), Vulnerability Scanning (3.11.2), Reviewing and update logged events (3.3.3), Alerting on audit process failures (3.3.4), Audit record review, analysis, and reporting processes (3.3.5), Testing of incident response capabilities (3.6.3), Establishing and maintaining baseline configurations (3.4.1)
- **DIBCAC discovered that 38% of all organizations receiving assessments have failed to adequately deploy Multi-Factor Authentication. In some of these cases, implementation attempts were made but did not completely cover the assessment scope**.
- If an organization has deployed FIPS validated Encryption mechanisms where the cryptographic module certification has expired; DIBCAC is not considering this as the organization completely failing to meet the expectation. Instead, these organizations will be granted an “other than satisfied” determination due to a temporary deficiency that is out of their control. The OSC will need to POAM this control and may receive partial credit (3/5 points) for the control.
- **DIBCAC conducted an analysis of all SPRS submissions and found that the average score of all organizations was 66. The analysis also revealed an average increase of only 3 points in organizations submitting scores for a second time**.
- DIBCAC also analyzed medium-level assessments between 07/2021 and 03/2022 and found 156 instances where the score reported decreased by at least 100 points when validated by DIBCAC. This includes one case where a contractor had an SPRS score of 110 (best possible) but was validated with a score of –203 (worst possible).
- **The average SPRS submission of all organizations in the study was 56.125; the average of the medium assessment scores of those same organizations was –57.25.**
- 26% of all self-attested “basic assessment” scores submitted were 110
- 79% of all organizations receiving a medium assessment received a score of 110
- 49% of organizations who participated in a DIBCAC High assessment received a score of 110.
- In a comparison of the scoring of Basic to Medium assessments. A slide representing the actual scores of 16 contractors was provided. Only 1 set of contractor data showed an improvement in scores between their basic and high assessment. Only 2 scored above 50 on their medium assessment. **And 7 of the 16 contractors saw self-attested scores of 50+ turn into validated scores of negative values.**

The Department of Defense (DoD) was instructed in National Defense Authorization Act FY 20 Section 1648 – Framework for Protecting the Defense Industrial Base. One of the core tenants of the 1648 report was to establish and ensuring compliance standards, regulations and polices and to deconflict existing cybersecurity standards, regulations and polices. The DoD had already started with the Cybersecurity Maturity Model Certification (CMMC). The CMMC is a matrix of all of the various cybersecurity standards that streamlines and deconflicts for industry what is needed to be complaint. The CMMC program is run currently out of the DoD Chief Information Office under the Chief of Defense Industrial Base Cybersecurity.

The CMMC is also what was called out as a need in the Cyberspace Solarium Commission (CSC) report about a National Cybersecurity Standard as stated in section 4.4.3 Incentive Information Technology Security through Federal Acquisition Regulations and Federal Information Security Management Act Authorities. In which the bi-partisan reports states to use and build upon the CMMC. The report states, "Requiring vendors to adhere to standards when doing business with the federal government will compel them to produce products or service offerings that meet those standards, potentially making those more secure offerings available to the broader public."

Assumptions based on research by several industry components have made conclusions about what amount of funding is needed to ensure security and compliance. In the NDAA FY20 Sec 1648 report it was requested that that DoD identify the cost of compliance and timelines for implementation. This is difficult for the DoD to accomplish and publish in the 1648 report as they are in the process of the DFAR rule change and puts them at risk of not following the law during this process.

Assumption:

The cost estimate is based on the DIB wide Small to Medium (SMB) suppliers to comply with CMMC 2.0 Level 2. This would be known as Cybersecurity as a Service (CSaaS) as most of the DIB does not currently have the capability to provide this organically in their firms. This may change over time, but until pilot programs are started this analysis is very close to what we understand as of today in respect to where the DIB is in compliance.

DIB Construct:
80K Companies which equals about 8M seats

SMB (1-500) employees which are about 90% of the DIB
SMC (500-5,000) Employees which are about 8% of the DIB
Enterprise (5,000 – Up) Employees which are about 2% of the DIB

Included in the One-Time cost analysis:

SSP Development / Policy / Procedure Development
Office 365 Implementation to CMMC L2
Azure Implementation to CMMC L2

- MFA to the Desktop built to CMMC L2
- Migration (Users, Email, SharePoint, OneDrive, Teams) to GCC High
- Managed Services Onboarding
- Managed Security Services Onboarding
- 3rd Party Assessment (C3POA)
- Assessment Support

Included in Yearly Licensing / Subscriptions:

- MS365 E5 Licensing
- Azure Subscription for the Azure Infrastructure and Duo Implementation
- Duo Federal

Included in Monthly Costs (Operations):

- Managed Services for Full Users
  - M365 Infrastructure Support
  - Mobile Device Support
  - Full Desktop Support
  - Full 24 x 7 helpdesk
- Managed Services for Infrastructure
  - Firewall Management
  - Server Management
  - Azure Infrastructure Support
  - Microsoft Premier Support
  - Full 24 x 7 NOC
- Managed Security Services
  - SIEM Management
  - Vulnerability Management
  - Intrusion Detection / Incident Response
  - Threat Feed Integration
  - Full 24 x 7 SOC

Fully Burden Costing:

This will range from (low) $1,900 to (high) $7,400 cost per seat depending on size of firm and complexity of work.

So, if we assume there are 8M seats in the DIB, and an average cost of $5,000 a year for security a Rough Order of Magnitude (ROM) would be 40B.

If appropriations would provide $10B +/- to be given directly to the DoD CIO Chief of DIB Cybersecurity to be provided to the appropriate military service acquisition program as they implement the new DFAR rules 7020, 7021 and 7022, every year for the next 5 years to get to where we need to be to provide required cybersecurity to our nation. At a bare minimum there is a need of at least $30M to fund the pilot programs in 2023. This would be a one-time plus up to level set what is needed. This would also allow for Office of Management and Budget along with DoD to complete the appropriate analysis to ensure these measures and standards are providing the taxpayer a return on investment.

The return on investment (ROI) for Congress to fund this is paramount, as we are losing billions of dollars a year that will never be recovered or made up in research. We fund Ukraine to fight a war against Russia, but we won't fund our own cyberwar with the multiple adversaries that are at with us in a non-kinetic method daily. Sen Joanie Ernst last week was surprised to see that a SBIR was compromised, the Defense Industrial Base is hit daily with ransomware is up across the world, other US agencies have been hit, schools, airports etc. When is enough going to be enough?