

ICIT'S BRIGHT MINDS Q&A SERIES



SMB Cybersecurity in the Defense Sector

with

ERNIE MAGNOTTI CISO, LEONARDO DRS

November 2019

ICIT | Institute for Critical
Infrastructure Technology
The Cybersecurity Think Tank

 **LEONARDO DRS**

ICIT's Bright Minds Q&A Series

The Role of SMBs on DIB Cybersecurity

With Ernie Magnotti, CISO, Leonardo DRS

November 2019

Copyright 2019 Institute for Critical Infrastructure Technology. Except for (1) brief quotations used in media coverage of this publication, (2) links to the www.icitech.org website, and (3) certain other noncommercial uses permitted as fair use under United States copyright law, no part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For permission requests, contact the Institute for Critical Infrastructure Technology.

About This ICIT Bright Mind Q&A

In continued support of our mission to cultivate a cybersecurity renaissance that will improve the resiliency of our nation's 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders, ICIT has embarked on a journey to hold candid interviews with some of the brightest minds in national security, cybersecurity, and technology. Our goal is to share their knowledge and insights with our community to shed light on solutions to the technology, policy, and human challenges facing our community. Our hope is that their words will motivate, educate, and inspire you to take on the challenges facing your organizations

This Bright Minds Q&A featuring Leonardo DRS CISO and ICIT Fellow Ernie Magnotti adds to the research already published as part of ICIT's [Improving Supply Chain Resiliency](#) initiative by discussing America's national security prerogative to improve supply chain security within the defense industrial base and whether the U.S. Department of Defense's (DoD) Cybersecurity Maturity Model Certification (CMMC) is sufficient to catalyze improved cybersecurity.

MITRE's late 2018 report *Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War*, [summarized by ICIT here](#), found the vast majority of government contractors were not meeting the requirements of DFARS 7012, and many more did not have the understanding or means to meet the regulations. The report calls for security, in addition to cost, performance, and schedule, to be the primary determinants in the acquisition process.

The CMMC is the DoD's attempt to apply the findings of the *Deliver Uncompromised* study to the defense industrial base (DIB) supply chain. The CMMC is a cybersecurity assessment model and certification program that was introduced by the DoD to secure the DIB, and as such will apply to all contractor and subcontractors within the DIB. Contractors are evaluated based upon the implementation of actual technical controls in addition to their documentation and policies. These evaluations lead to a level certification of 1 (least secure) to 5 (most secure). The higher a company certifies, the more contracts they will be eligible to bid on. The CMMC level requirement will flow down to all subcontractors. Additionally, future request for proposals (will require a CMMC level regardless of whether they handle controlled unclassified information or not.

In this Bright Minds Q&A, Ernie Magnotti explains how he believes the CMMC will cause the sector to evolve, inviting a cybersecurity renaissance into America's DIB.

About this Bright Mind: Ernie Magnotti, CISO, Leonardo DRS



Ernie Magnotti is the CISO with Leonardo DRS, a \$2.5 billion cleared defense contractor of 6500 employees headquartered in Arlington, Virginia. In this role, Ernie leads the DRS Cyber Security program, providing all aspects of information assurance, including detection, response, compliance, governance and risk management. As a strong believer in industry collaboration, Ernie personally supports cyber security outreach opportunities wherever possible, especially downstream in the supply chain of the Defense Industrial Base. Ernie also believes in the importance of cyber awareness, and spends considerable time traveling to DRS manufacturing sites nationwide providing in-person training to DRS employees. Ernie is a CISSP-ISSMP, a certified ITIL Expert, and holds a master's degree in cyber security from Valparaiso University.

In 1997, Ernie launched a web development/hosting company, and he's been in IT operations and cyber security ever since. In 2006, he joined Leonardo DRS as an IT operations manager and quickly moved up in the organization to fill critical roles in IT and cyber security. He became the DRS CISO in 2014 after he led the consolidation of DRS IT in 2013. As DRS CISO, Ernie established the DRS cyber security program growing it to become a critical element of DRS's award-winning industrial security program.

A seasoned professional, Ernie has more than 34 years of experience in telecommunications. Throughout his career, Ernie has worked for companies of all sizes, from his Internet startup to as big as Microsoft. This gives Ernie the perspective to understand the subtle impacts of IT on businesses, from both "enabling" and "securing" paradigms.

In addition to a master's degree in cyber security, Ernie received an his undergraduate in Radio and Television from the University of Arizona. He worked as a sales engineer for Sony for over 10 years, providing broadcast television equipment to television stations across the U.S. As a sales engineer, Ernie honed his skills in business acumen and persuasion, which has served him well in his technical leadership roles throughout his career.

Ernie and his wife Terri have been married over 30 years. They live in the Dallas area. They have two children: Zachary, a senior at Texas A&M University and Shelly, a sophomore at Edward S. Marcus High School. Ernie and his family enjoy traveling together, especially to the Rocky Mountains where they love to hike, ski, and Jeep. Ernie is also an avid fresh water fisherman.

ICIT:

How would you describe the composition of the defense industrial base (DIB) third-party ecosystem? In your opinion, what aspects are underreported and what are the resulting impacts on supply chain security?

Ernie Magnotti:

According to [Aeroweb](#), the top 100 Defense Contractors accounted for 63.5% of the prime contracts awarded in 2018, with the top 6 accounting for 30% of the total. But naturally, the Department of Defense (DoD) begins to lose sight of subcontractors beyond the third tier of the supply chain. I've heard estimates that there are between 100k and 300k companies holding contracts with DoD flow downs, approximately 98% of these companies have fewer than 100 employees, and there are over a million contracts in the DIB ecosystem that contain DFARS clause 252.204-7012.

DFARS clause 252.204-7012 requires that data breaches involving controlled unclassified information (CUI) be reported through DIBnet. However, the clause and associated requirements are not easy to understand, and companies with fewer than 100 people might have one to three IT people who mainly do break/fix work, leaving them with little manpower for cybersecurity. Thus, it's very likely that small companies do not have a sophisticated cyber program capable of defending against nation state threat actors, let alone understand how to comply under the clause. This is why the bad guys are focusing their cyberattacks further down the DIB supply chain.

ICIT:

What risks do small contractors introduce to the DIB ecosystem when they cannot meet the security requirements set by the government or when the minimal requirements are insufficient to mitigate emerging threats?

Ernie Magnotti:

In June 2019, the DIB announced an aggressive plan to require a [Cyber Maturity Model Certification \(CMMC\)](#) for all contractors and subcontractors that will require an independent third party to assess a company's cyber maturity before they can win contracts that contain DFARS clause 252.204-7012. Many in the DIB are concerned that the CMMC introduces new risks in the supply chain due to smaller companies' inability to meet necessary maturity levels. On the other hand, the intent of the CMMC is to simplify the number of cyber requirements necessary for smaller companies. The DFARS clause requires companies to meet 110 requirements for each information system, but, under CMMC, smaller companies will only need to meet a focused subset of the 110 controls to be eligible for contracts. The net-net is that by narrowing the number of requirements and using 3rd party assessments, subcontractors will focus on lower maturity cyber-hygiene.

To restate, the DIB needs the smaller contractors to build a foundation that deliberately focuses on cyber-hygiene. For example, are we doing timely patching? Do we have good endpoint

protection? Are we ensuring robust access management to important information systems? Do we have robust gateway protection with multifactor remote access?

Consider a small company that has outsourced software development. This might come as a surprise to some people, but software developers are not usually concerned with secure software development. It's easy to imagine a well-resourced threat actor dwelling in such a company's network indefinitely, inserting malicious code to achieve their objectives. Extend this consideration to small companies who make programmable devices, often aggregating those devices from several sources. How were those devices tested for integrity? How do we ensure the devices weren't tampered with while in transit from the subcontractor? When you think about software code or programmable devices sourced from small companies, it's easy to imagine how they can be compromised. The government's minimal requirements are not yet enough to mitigate these existing threats.

ICIT:

On July 25, 2019, the DOD Inspector General released [a report](#) which concluded that many defense contractors were failing to secure sensitive information because, among other shortcomings, they did not employ multifactor authentication, enforce strong password use, identify and mitigate vulnerabilities, or document and track cybersecurity incidents. How widespread would you estimate these deficiencies are?

Ernie Magnotti:

There are so many interesting and alarming reports about DoD cyber deficiencies. Another report published by [Sera-Brynn in May of 2019](#) estimates that companies of greater than \$500 million revenue average only 60% of full implementation of the 800-171 controls. They also identified 16 specific controls that are consistently not fully implemented, including multifactor authentication. Yet another article published by GAO in October 2018 about "[DoD Just Beginning to Grapple with Scale of Vulnerabilities](#)" discussed the need for greater defense contractor security.

I believe the deficiencies are universal, and they exist, to some degree, inside every contractor. For instance, the major contractors have complicated information systems that are not necessarily under central control. Or, as you move further down in contractor size, the depth of cyber resources becomes proportionally fewer as the information systems become less complex. All contractors, just like all companies, have cyber deficiencies, but the types of deficiencies are unique to each contractor due to size, culture, business model, etc.

ICIT:

How do the requirements of [NIST Special Publication 800-171 Rev. 2](#) and [SP 800-171B](#) impact smaller DIB contractors? How might these special publications shape the DIB in the future?

Ernie Magnotti:

These requirements do add to the confusion for small contractors. The reference 800-171B might be considered the next revision of 800-171A, but 800-171A is an assessment guide for 800-171r1 while 800-171B is an additional set of enhanced requirements that can be applied ad-hoc depending on the sensitivity of the contract. It's like trying to explain CUI, which is a classification that is unclassified; does that make sense to you? The DFARS clause refers to safeguarding covered defense information (CDI), and to do it using 800-171, which is guidance for safeguarding controlled unclassified information (CUI). Now try explaining this to a company executive, who we're asking to support the inconveniences and costs of CUI safeguarding. It's hard enough to explain this to executives at a billion-dollar company, let alone smaller businesses.

I'm hopeful that the DoD's new CMMC approach will do more to help communicate requirements to smaller companies. As I said earlier, the intent of the CMMC is to simplify the approach for smaller contractors.

ICIT:

Will [CMMC](#) increase the cybersecurity posture of the DIB? How will contractors respond to the CMMC?

Ernie Magnotti:

Yes, it will definitely increase the posture. It's going to have a strong positive impact once we work through the wrinkles, which won't be easy. But industry is already showing a very positive reaction. There is a strong collaborative effort between industries and the DoD, as they both want to do this right and quickly. The outcome will be a certification score. If your score isn't high enough, you can't compete for programs. That's easy to explain to executives. There is also the benefit of removing subjectivity from assessor methodology and significantly reducing the number of assessments from DoD and industry alike.

ICIT:

What do small businesses need to do to remain compliant in the DIB?

Ernie Magnotti:

As far as the 7012 clause and what companies should be doing to be compliant, I suggest they join the DIB and attend the quarterly meetings. The perspectives gained at the DIB meetings are critical to keeping up with the moving target of cyber compliance and helping companies

work through the confusion. Through the DIB, small businesses can collaborate with bigger contractors and learn from their experience and perspectives. More information about the DIB is available at <https://dibnet.dod.mil>. The hot topic at recent DIB meetings has been the CMMC, so attending the DIB quarterlies is an effective way to hear the latest information and get in front of the coming requirements.