security current

Aligning Corporate Executives with US Federal Government Regulations Associated with Contractor and Supply Chain Security Requirements

by DARREN DEATH

A CISOs Connect Report

TABLE OF CONTENTS

Introduction 3

Recent US Federal Government Cybersecurity Timeline 3

Cybersecurity should be viewed as a strategic investment 5

Understanding the problem 7

Organizational Change Management 9

Technical Debt 9

References 10

About the author 12

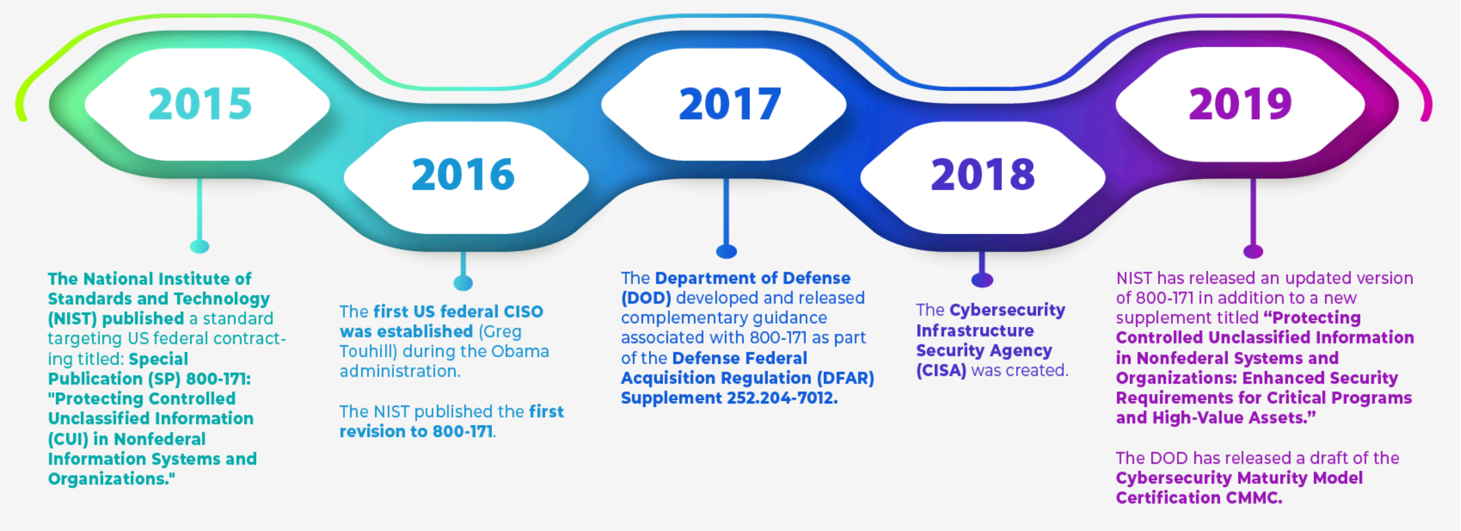
INTRODUCTION

There has been an uptick in the federal government's focus relative to requirements imposed on federal contractors regarding securing their information systems, In September 2018 I wrote an article titled Information Security Requirements for US federal contractors that focused on NIST 800-171 and the federal government's attempt to manage third party risk by implementing government contractor security requirements (Death, 2018).

Cybersecurity is playing a pivotal role in US federal government modernization which has evolved significantly in regard to its oversight and guidance. Legislative and regulatory changes have been made within the federal government and externally towards the federal government's supply chain. The federal government has established and is continuing to refine standards that are related to information security requirements that serve to establish the government's protection requirements for sensitive government information that reside on contractor networks.

To gain a better understanding of the government's approach to contractor security, it is important to take a brief look at that past few years and observe the progress that the government has made in setting cybersecurity standards.

Recent US Federal Government Cybersecurity Timeline



2015

The National Institute of Standards and Technology (NIST) published a standard targeting US federal contracting titled: **Special Publication (SP) 800-171: "Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations."**

2016

The **first US federal CISO was established** (Greg Touhill) during the Obama administration.

The NIST published the **first revision to 800-171**.

2017

The **Department of Defense (DOD)** developed and released complementary guidance associated with 800-171 as part of the **Defense Federal Acquisition Regulation (DFAR) Supplement 252.204-7012.**

2018

The **Cybersecurity Infrastructure Security Agency (CISA)** was created.

2019

NIST has released an updated version of 800-171 in addition to a new supplement titled **"Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High-Value Assets."**

The DOD has released a draft of the **Cybersecurity Maturity Model Certification CMMC.**

2015
The National Institute of Standards and Technology (NIST) published a standard targeting US federal contracting titled: [Special Publication (SP) 800-171 in 2015 titled: "Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations."]()

2016

The first US federal CISO was established (Greg Touhill) during the Obama administration, to develop and champion a cybersecurity strategy that required the implementation of safeguards and the development and implementation of strategy related to effective information sharing across agencies.

The NIST published the first revision to 800-171 in 2016.

2017

The Department of Defense (DOD) developed and released complementary guidance associated with 800-171 as part of the Defense Federal Acquisition Regulation (DFAR) Supplement 252.204-7012. This supplement requires the implementation of 800-171 requirements on contractor networks that support the DOD and host covered defense information (CDI).

2018

The Cybersecurity Infrastructure Security Agency (CISA) was created with the goal of leading cybersecurity protections throughout the federal government. Additionally, CISA is charged with working with the private sector to ensure better intellectual property protections and a more secure critical infrastructure.

2019

NIST has released an updated version of 800-171 in addition to a new supplement titled "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High-Value Assets." This is used for organizations that are processing high value data on contractor information systems.

The DOD has released a draft of the Cybersecurity Maturity Model Certification CMMC. This standard removes the self-attestation process related to 800-171 and brings in a third party that reports contractor security accomplishments to the government through an auditing mechanism.

Upon review of this timeline, it is evident that the federal government is increasing its focus on cybersecurity. Based on this, ***the government contracting communities' senior leadership should conclude that these requirements are not going away and that they will be required in order to perform work for the government in the near future.***

Cybersecurity should be viewed as a strategic investment

Cybersecurity should be treated as a strategic investment by the government contracting organization (Mithas & Rust, 2016). A strong cybersecurity focus serves to ensure that an organization is resilient and that it can resist a cyberattack that could result in lost productivity, business disruption, intellectual property theft, and/or brand damage. Additionally, implementing these capabilities serves to ensure that the government contracting organization remains competitive. The recently released CMMC guidance from the DOD states that the requirements laid out in the standard are expected to be included in requests for proposals by the end of 2020. This creates an environment where a company could be unable to compete due to not establishing the needed cybersecurity controls required by a specific contract. This sets the stage for a strategic business need by the contracting organization to establish a cybersecurity program that meets government requirements and establishes a framework for the organization that helps to ensure its resiliency.

A close relationship with the organizations' senior leadership is necessary to ensure that the cybersecurity program is properly supported as a strategic investment and is aligned across the organization (Rothrock, Kaplan, & Oord, 2018). This focus helps to ensure that cybersecurity initiatives receive the support and attention needed to meet the government's requirements. Securing this commitment from senior leadership is vital in that the changes required to implement an effective cybersecurity strategy within an organization requires that the organization has the appropriate funding and approvals.

Setting the stage early with organizational executives will help to ensure program success when new capabilities being implemented may be considered disruptive to the business and by team members throughout the organization. Having the support of the senior leadership team helps to ensure that the conversation is not "do we do this?" but is rather "how do we do this?"

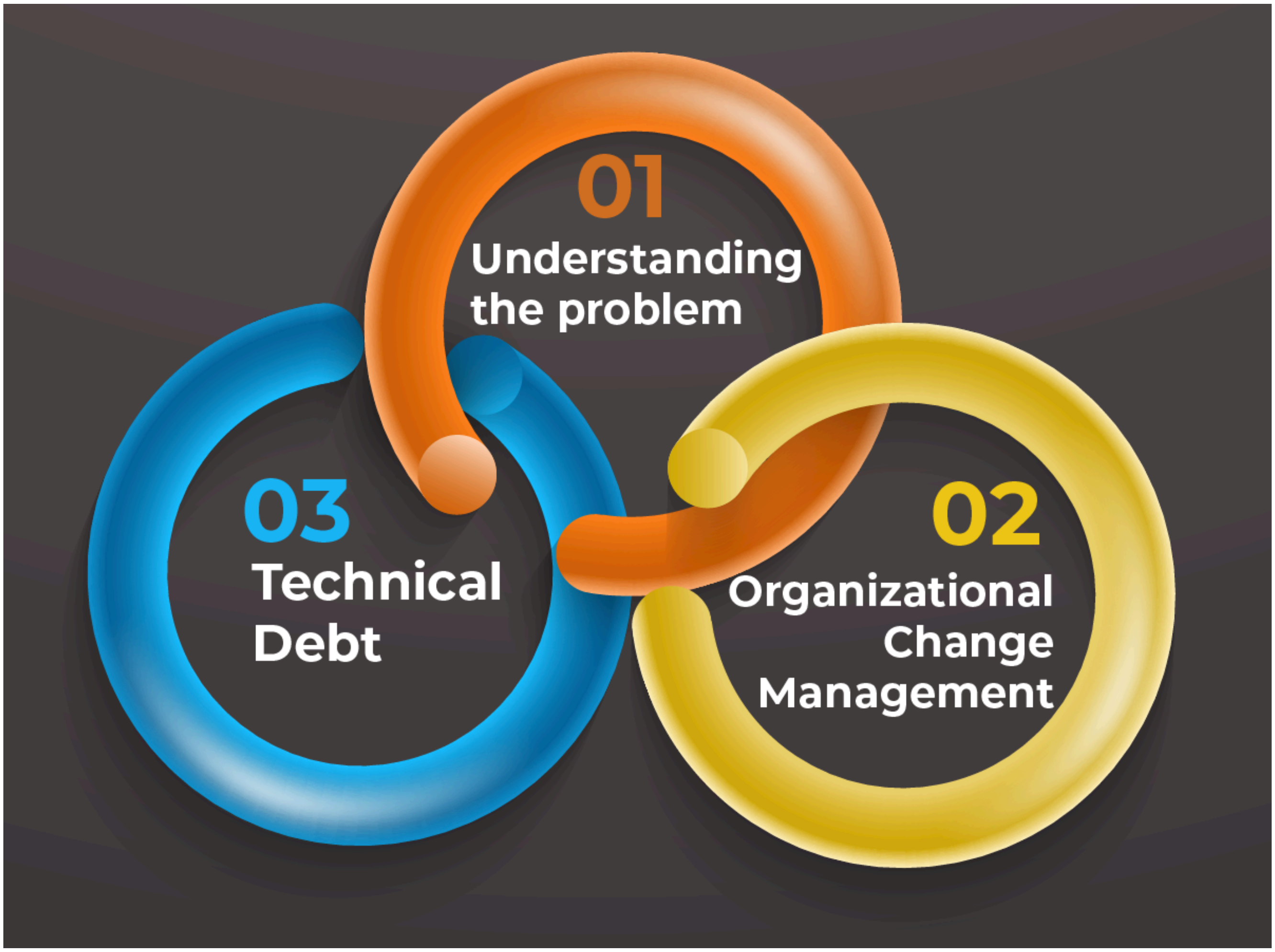
It is important that you do not simply rely on the credibility of your senior leadership team. You must ensure that you establish effective communication throughout your organization related to changes that will be made to support cybersecurity improvements (Tang, Li, & Zhang, 2016). If you are simply relying on the apparent buy-in of the senior leadership, you will find that the mood of the business may change as organizational change becomes more complicated. As a result, it is critical that you implement effective organizational change management practices that communicate the need and benefit of the cybersecurity changes being implemented across the organization.

Establishing an effective organizational change management practice combined with effective support from your company's leadership will provide you with the tools to manage and communicate the changes that will be occurring throughout the organization in response to federal cybersecurity requirements (Hornstein, 2015). It is vital that the CISO communicate effectively throughout all levels of the organization regarding changes that are being made to the organization, and how those changes will benefit the organization, help to ensure resilience, and protect the jobs of the affected employees.

Cybersecurity must be well aligned with the organization's mission (Sabherwal et al., 2019). Being able to implement the solution that ensures that contracts are not in jeopardy because of cybersecurity non-compliance is a perfect example of aligning the cybersecurity program strategically with the needs of the business. While the standards published by the government have not seen mandatory adoption, a review of historical contract data over the past year has shown that the government is implementing contracting language that requires the implementation of 800-171 and ISO27001 controls as part of contracting language and requirements.

It is also important to remember that cybersecurity requirements may not simply come from the federal government. Prime contractors can impose security requirements on their sub-contractors as part of their teaming and sub-contractor agreements that meet or exceed the federal government's requirements. In the case of government and prime contractor-imposed cybersecurity requirements, the implementation of an effective risk-based cybersecurity program is table stakes for entry to many contracts and establishes a clear case for a strategic approach to implementing cybersecurity within the government contractor.

Areas to focus on that will help to ensure that cybersecurity is taken seriously within your organization



Understanding the problem: Understand that the cybersecurity issue facing the government contracting leader is not specifically associated with resilience or security (While it should be a major focus). In order to remain competitive in the government-contracting arena, the contractor is going to need to focus on cybersecurity capabilities to ensure that they qualify to compete for new contracts. Cybersecurity requirements are being written into individual contracts and they will eventually be mandated across the government. Handling these new cybersecurity requirements is the problem facing government contracting leadership and focusing on solving this competitiveness problem should be the focus of the CISO, C-Suite, and Board (Sabherwal et al., 2019).

Focus on investment: Now that the problem is well understood, the CISO should focus on how investing in cybersecurity is a strategic move for the government contractor as this investment will serve to support the continued ability of the company to go after contracts that have a cybersecurity requirement as a barrier to entry (Morrison & Kumar 2018). As part of the investment conversation, the CISO must discuss how developing these new capabilities do not simply serve to assist with contract competitiveness, but also serve to ensure corporate resilience. In this way, the CISO is using compliance (typically a dirty word) to align with business objectives and to ensure a resilient and enduring operating capability for the company. However, while actively implementing these federal requirements, the focus should be on security and not checkbox compliance. ***Implement secure solutions for your organization that serve to protect your company and in turn serve to meet the government's requirements.***

It is also important to ensure that while you are establishing or expanding your cybersecurity program, you not only focus on compliance but that you also focus on organizational risk. As mentioned above, the capabilities that are implemented by the organization must ensure a secure organization. This is a better approach than ensuring a compliant organization that is woefully insecure. This means that a couple of tactics should be implemented while establishing your cybersecurity program. First, you must effectively triage your organizational environment. This means that you must understand what is critical and foundational to implementing within your organization. Implementing those capabilities first in order to close serious vulnerabilities can eliminate or greatly reduce threats to the organization. Remember that risk ownership is owned by the senior most individuals of your organization. Continue to communicate and maintain support with these leaders as you establish the cybersecurity program to ensure that risk is properly mitigated.

It is also important to take a maturity approach when implementing new cybersecurity services within the organization. This means that you should implement a crawl, walk, run approach to implementing these new capabilities. Initially, you may implement a capability that meets requirements and is secure but is manual in nature using already existing network-based instrumentation. Over time, you may move to a more mature approach that uses a more automated approach that combines the outputs of multiple tools in an automated fashion to create new knowledge that can be used to increase visibility and reaction time to an intrusion (Death 2019, August). In this way, you can plan a risk-based strategy for a cybersecurity program that takes the organization's risk appetite into account while maturing over time to meet ever changing challenges.

Organizational Change Management: It is important that the CISO "hit the streets" in order to conduct an effective marketing campaign throughout the company. Many stakeholders exist related to this problem. The CISO should be working throughout the organization to communicate the need for effective security capabilities (Death 2019, February). As an example, contracts and business development organizations are keenly aware that they need to meet governmental cybersecurity requirements to surmount any barrier to entry and stay compliant with government mandates. Work with leaders in these organizations to make a case and develop champions who can support your cybersecurity effort. Work with your C-Level executives and board members to help them understand how implementing these new capabilities will assist in showing a strong commitment to customers, ensures organizational resiliency and serves to meet requirements needed to compete. Show organizational users how new cyber capabilities serve to protect the organization and their jobs. ***By communicating in this way, the CISO is developing a role-based strategy that targets needed cybersecurity capabilities in a way that connects with the specific audience.***

As a responsible organization, the implementation of security controls serves to support the organization and its users. While communicating with your audience, the focus should not be on technology. Rather you should be focusing on the business problem presented by the government. The problem can then be discussed relative to how the cybersecurity program with other parts of the business will work together to solve this problem in business terms (Stewart & Jürjens, 2017). Focusing on technical details may lead to confusion and can result in disinterest. This, in turn, may lead to any new cybersecurity efforts being seen as superfluous as they do not support the mission of the organization.

Technical Debt

Now is a great time to discuss technical debt. As mentioned previously, these requirements are not new, and the government is continuing to increase their vigilance related to government contractor's cybersecurity. If a cybersecurity program has not begun following the requirements provided previously by the federal government it has now become more urgent due to potentially impeding and more stringent requirements. The contractor will now need to move faster and work with other vendors whose time is now at a premium. Essentially, waiting to work on an effective business-aligned cybersecurity program has resulted in a program that is now more expensive to implement because vendor and partner resources required to compete cybersecurity projects cost more due to supply and demand constraints (Shein, 2018). Additionally, the organization may be unable to compete on contracts that they are qualified for because of non-compliance. ***It should be expected that these requirements are not going away and any further waiting to invest will only result in further technical debt being accumulated by the organization.***

The bottom line for the government contractors is that federal cybersecurity requirements are not going away and the threats against the government contractor are very real, considering the sensitive information they may possess. Considering this, it is vital for the government contractor to plan and implement a cybersecurity strategy that meets the federal government requirements while ensuring a secure and resilient outcome for the organization.

REFERENCES

Death, D. (2018, September 4). *Information security requirements for U.S. federal contractors.* Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/09/04/information-security-requirements-for-u-s-federal-contractors/

Death, D. (2019, February 18). *Must have skills for CISOs: a CISOs Connect report.* Retrieved from https://securitycurrent.com/must-have-skills-for-cisos-a-cisos-connect-report/

Death, D. (2019, August 20). *Is cybersecurity automation the future?* Retrieved from https://www.forbes.com/sites/forbestechcouncil/2019/08/20/is-cybersecurity-automation-the-future/

DOD. (2019, June 28). *Defense federal acquisition regulation supplement 252.204-7012.* Retrieved from https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm

DOD. (2019, September). *Cybersecurity maturity model certification.* Retrieved from https://www.acq.osd.mil/cmmc/draft.html

Hornstein, H. A. (2015). The integration of project management and organizational change management is now a necessity. *International Journal of Project Management, 33*(2), 291-298. doi:10.1016/j.ijproman.2014.08.005

Mithas, S., Rust, R. T. (2016). How information technology strategy and investments influence firm performance: conjecture and empirical evidence. *MIS Quarterly, 40(1),* 223-245. doi:10.25300/MISQ/2016/40.1.10

Morrison, A., & Kumar, G. (2018). Corporate boards may be more likely than regulators to scrutinize cybersecurity program effectiveness this year: New Deloitte poll shows one third of executives plan to adopt AICPA's SOC for cybersecurity framework. Journal of Health Care Compliance, 20(4), 49.

Ross, R., Dempsey, K., Viscuso, P., Riddle, M., & Guissanie, G. (2018, June 07). *Protecting controlled unclassified information in nonfederal systems and organizations.* Retrieved from https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

Ross, R., Pillitteri, V., Guissanie, G., Wagner, R., Graubart, R., & Bodeau, D. (2019, June). *Protecting controlled unclassified information in nonfederal systems and organizations: enhanced security requirements for critical programs and high-value assets.* Retrieved from https://csrc.nist.gov/publications/detail/sp/800-171b/draft

Rothrock, R. A., Kaplan, J., & Oord, F. v. d. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review*, 59(2), 12-15.

Sabherwal, R., Sabherwal, S., Havaknor, T., & Steelman, Z. (2019). How does strategic alignment affect firm performance? the roles of information technology investment and environmental uncertainty. *MIS Quarterly*, 43(2), 453-474. doi:10.25300/MISQ/2019/13626

Scott, T., & Daniels, M. (2016, September 8). *Announcing the first federal chief information security officer.* Retrieved from https://obamawhitehouse.archives.gov/blog/2016/09/08/announcing-first-federal-chief-information-security-officer

Shein, E. (2018, November 14). *Security is everyone's responsibility*. Retrieved from https://www.cshub.com/security-strategy/articles/security-is-everyones-responsibility

Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information and Computer Security, 25*(5), 494-534. doi:10.1108/ICS-07-2016-0054

Tang, M., Li, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management*, *17*(2), 179-186. doi:10.1007/s10799-015-0252-2

Whitehouse.gov (2018, November 16). *President Donald J. Trump signed H.R. 3359 into law*. Retrieved from https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-signed-h-r-3359-law/

ABOUT THE AUTHOR

Darren Death

A proven technology leader with over 20 years of experience deploying enterprise systems for large private and public organizations, Death has led, designed, and implemented large-scale, organizational wide enterprise IT systems with far reaching impact.

Death currently serves on the EC-Council Global Advisory Board for TVM (Threat and Vulnerability Management) and serves as the InfraGard Maryland – Cyber Threat Special Interest Group Chief and American Council for Technology / Industry Advisory Council (ACT-IAC) – Cyber Security Community of Interest Program Chair.

Death serves on the Board of Advisors and as faculty for the Cyber Intelligence Initiative at the Institute of World Politics. Death holds a master's degree in Cybersecurity and Information Assurance and is currently working toward his Doctorate in Information Technology - Information Assurance and Cybersecurity.

This article aligns with Death's doctoral research in the field of Cybersecurity. Specifically related to the tools and techniques used by an organization in implementing a strategy that is organizationally aligned and focused on security.

Security Current improves the way security, privacy and risk executives share information and collaborate to protect their organizations and their data. Security Current also runs CISOs Connect, a knowledge-sharing platform exclusively for CISOs. Its CISO-authored and peer-driven proprietary content and events provide insight, actionable advice and analysis giving executives the latest information to make knowledgeable decisions.