DoD Requirements Toolkit for Manufactures

Daniel Glover
Research Assistant
IT Solutions Center
University of Cincinnati
Cincinnati, OH 45206, USA
daniel.glover@uc.edu

Hazem Said, PhD
Director, School of IT
University of Cincinnati
Cincinnati, OH 45221, USA
hazem.said@uc.edu

Abstract
Small to medium sized manufacturers struggle with assessing compliance with the new DoD regulations. While these companies focus on staying competitive within the civil and military supply chains, regulations attempt to address the notion that security is only as good as the weakest link. The University of Cincinnati and TechSolve collaborated to develop a toolkit that assess cybersecurity risks based on National Institute of Standards and Technology (NIST) Special Publications (SP) 800-171 and recommend technical- and policy-strategies. This self-contained toolkit provides an affordable method for creating and monitoring risk profiles for manufactures interested in compliance.

Author Keywords
Contractor Systems; Controlled Unclassified Information; CUI Registry; Derived Security Requirement; Executive Order 13556; FIPS Publication 199; FIPS Publication 200; FISMA; NIST Special Publication 800-53; Nonfederal Systems; Security Assessment; Security Control; Security Requirement; NIST; Special Publication 800-171; DFARS Compliance; Department of Defense; DoD, Compliance, DoD Toolkit.

ACM Classification Keywords
K.6.5. Management of computing and information systems.

Introduction
The purpose of the Toolkit is to provide manufacturing companies a method that assists in the assessment of compliance with the NIST SP 800-171 controls – a set of 110 cybersecurity practices meant to safeguard Controlled Unclassified Information (CUI) required for contracts with the Department of Defense (DoD).

The original deadline for compliance has passed – December 31, 2017. To be compliant, contractors and sub-contractors for the DoD are required to have three documents:

- Plan of Action & Milestones (POA&M);
- Incident Response Plan (IRP); and
- System Security Plan (SSP).

Problem Statement
Many large companies have had the budget and necessity for Information Technology (IT) departments dedicated to network security. Since many of these companies are well known, they are natural targets for hackers. It has been, for some time, in their best interest to put in place many of the best practices that are covered in NIST SP 800-171.

Smaller companies, which are comprised mostly of subcontractors, still subject to the regulations, have found difficulty in not only finding information, but also understanding and implementing the controls. These networking practices have been less of a concern due to several factors such as corporate culture and company size. These companies, until now, have had relaxed security strategies - if any at all. This relaxed atmosphere is the reason for the regulation and the reason small to medium sized manufacturing companies will be impacted more than large companies.

NIST SP 800-171 is based off more stringent rules for Federal Agencies. They have been written in a way that allows companies to become compliant without specifically dictating details such as configuration, hardware and/or software. They realize one-size-fits-all is not a concept in IT.

So, there is a regulation meant to make information more secure – a noble pursuit. There are several large companies that have had the majority of the best practices in place for several years, but many smaller companies that are encountering increased costs and scrambling to comply, maintain their contract(s), while keeping costs in perspective. This creates a gap.

NIST isn't prescribing exactly how to implement the security controls and vendors have a responsibility to cost-effectively meet these requirements. Controls left to interpretation by contractors looking to keep costs as low as possible, which is their fiduciary responsibility, may have an impact on securing information – the spirit of the regulation.

Research Questions
DFARS compliance is a confusing endeavor for small to medium sized manufacturing companies. The regulation is causing an investment in an area of business previously neglected or seen as unnecessary. The DoD added this regulation to safeguard information being

held by third-parties. Can a toolkit help manufacturing companies reduce costs and increase security?

Research Methods

TechSolve, an Ohio MEP, partnered with Information Technology Solutions Center (ITSC) of the University of Cincinnati (UC) to develop a toolkit that assists their clients with the DFARS regulations. The program is consulting-based, which consisted of two pilot projects. These customers will provide feedback throughout the process to improve the process and ultimately develop a web application to facilitate the initial compliance and ongoing lifecycle of cybersecurity and compliance.

Research Contributions and Significance

If successful, the DoD will have non-identifiable analytics of compliance and employed methods. NIST will also have non-identifiable data for ongoing issues and have a way to push out updates and announcements. Prime contractors would have a method for communicating with sub-contractors. Sub-contractors will have a portal to manage compliance and TechSolve will be assisting manufacturing companies across the country to maintain compliance more effectively and efficiently.

References

1. Ron Ross; Patrick Viscuso; Gary Guissanie; Kelley Dempsey; Mark Riddle. 2016. SP800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (Rev 1). December 2016. National Institute of Technology and Standards (NIST), Gaithersburg, MD.

2. NIST. 2017. SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations (Rev 5). August 2017. National Institute of Technology and Standards (NIST), Gaithersburg, MD.