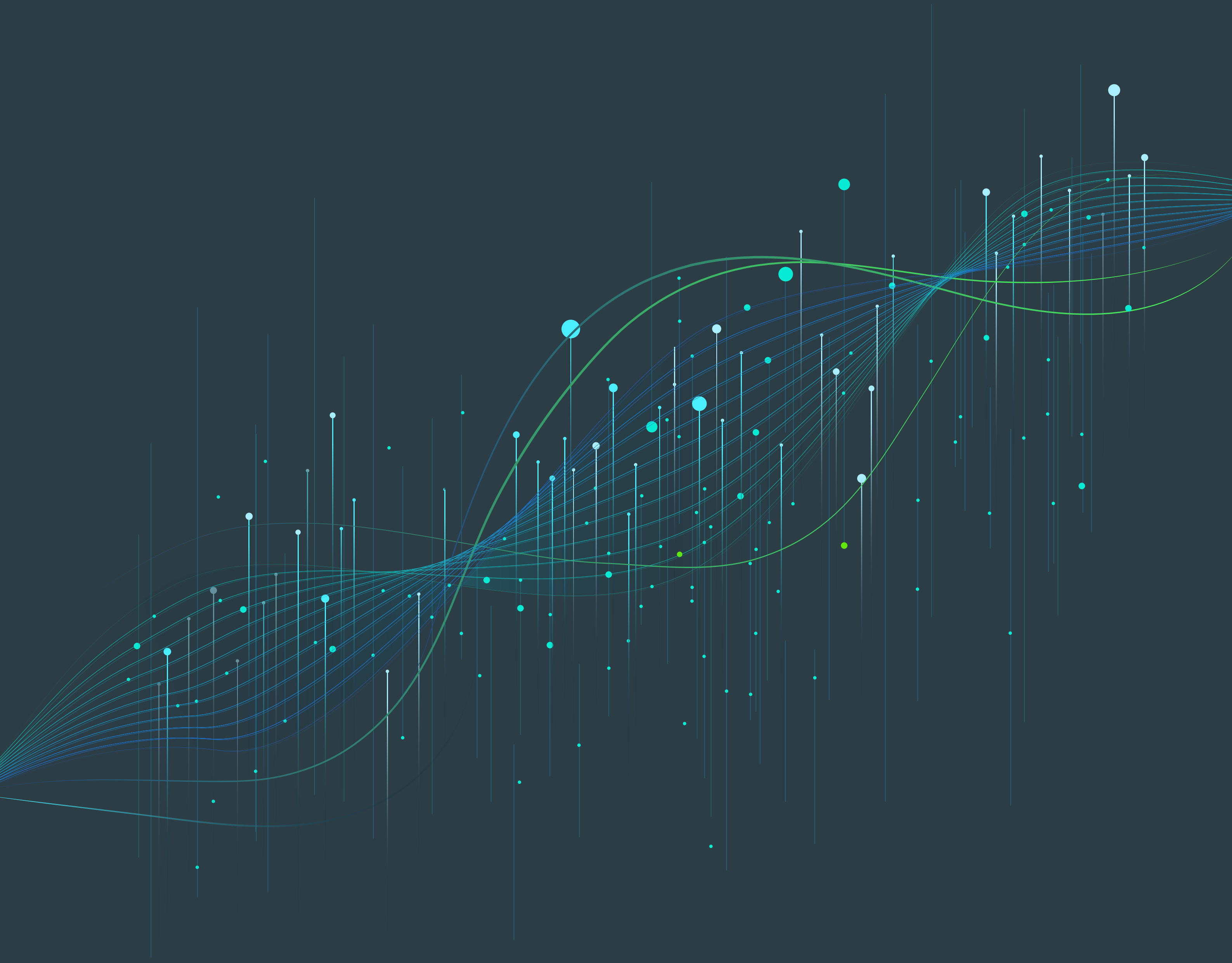
Reality check: Defense industry's implementation of NIST SP 800-171

Keen insights from certified cybersecurity assessors.

May 2019



SERABRYNN
GLOBAL LEADER IN CYBERSECURITY COMPLIANCE

As a certified auditor, Sera-Brynn has an inside look at how defense contractors are really doing when it comes to implementing cybersecurity acquisition clauses.

This report analyzes data compiled from two years of compliance assessments to identify areas where defense contractors typically fall short in implementing DFARS 252.204-7012 and the associated NIST 800-171 controls. While it provides a broad overview of industry's compliance with NIST SP 800-171 from an objective assessor's viewpoint, **the statistics presented here are likely optimistic.** Organizations assessed by Sera-Brynn already had concerns about DFARS and sought guidance to ensure compliance.

Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 implementation was supposed to be complete in December 2017 for any defense contractor subject to the contract clause. By mandating the implementation of National Institute for Standards and Technology (NIST) SP 800-171 and providing specific requirements for incident response and reporting, DFARS is intended to protect Controlled Unclassified Information, or CUI, and better secure the Department of Defense (DoD) supply chain.

A survey conducted by the National Defense Industrial Association found that less than 60% of respondents had read the cybersecurity clause and half of those found it hard to understand. About 45 percent of respondents had not read NIST 800-171 guidelines.[1] In contrast to NDIA's survey, our analysis was derived from assessments on contractors who were both aware of and motivated to implement the DFARS clause. In general, our findings paint a somewhat rosier picture than the survey, but the overall conclusion is the same: full implementation of NIST 800-171 remains a significant challenge.

Key Findings

Of the companies assessed:
- Zero companies were 100% compliant.
- On average companies implemented only 39% of the controls.
- 61% of the controls were either not implemented or only partially implemented.

[1] https://fcw.com/articles/2019/03/31/defense-supply-chain-weak-links.aspx?m=1

- Large companies, on average, successfully implemented nearly 60% of the controls.
- Small to mid-sized companies, on average, successfully implemented 34% of the controls.
- Over 80% of companies assessed failed to implement 16 specific controls.

The Not-So-Sweet 16 Controls

16 specific controls from the NIST 800-171 framework were consistently not implemented:

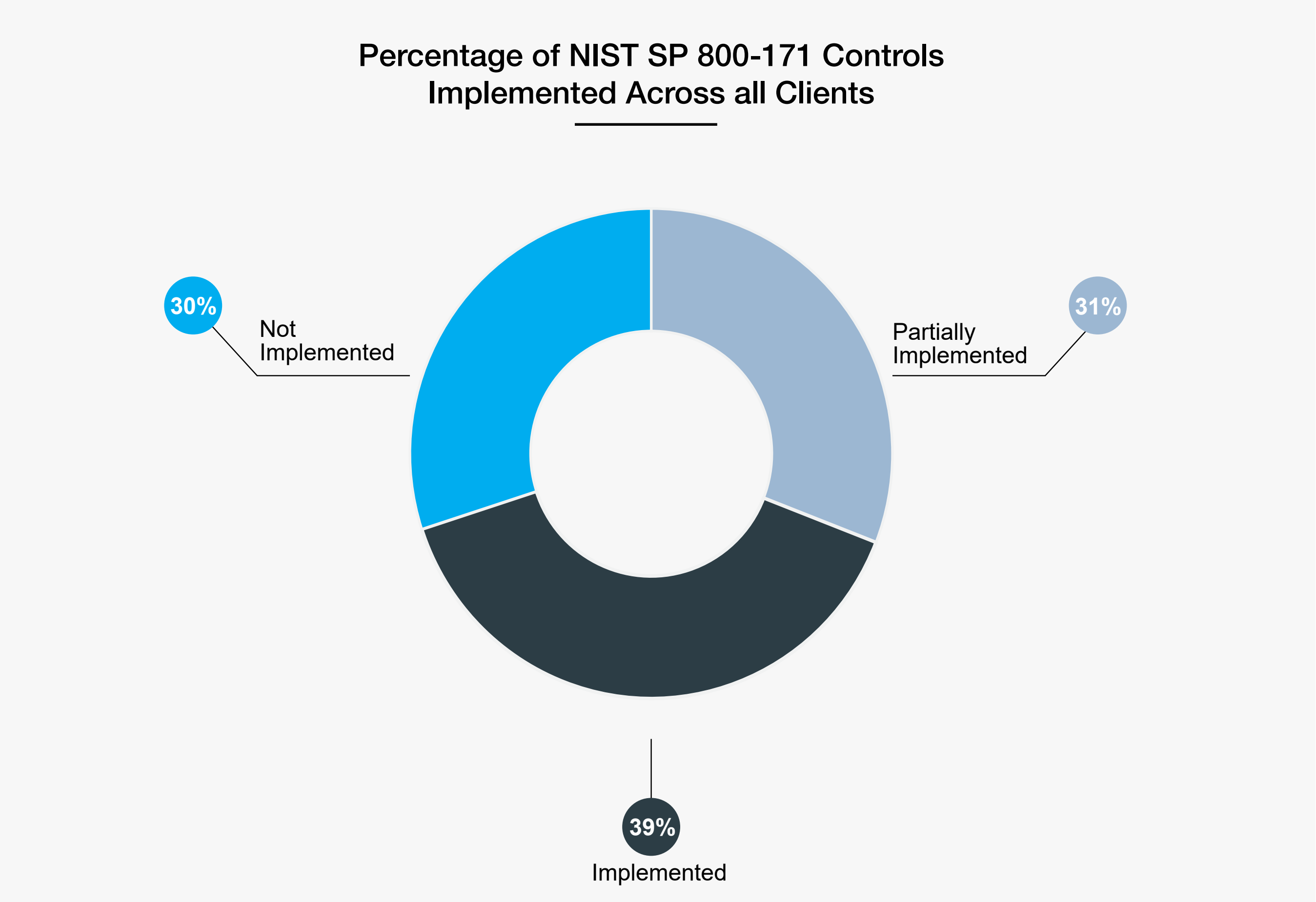
3.1.3 (CUI flow)
3.1.11 (session termination)
3.3.4 (audit log logging failure)
3.4.2 (configuration)
3.4.8 (black-/white-listing)
3.5.3 (multifactor)
3.6.3 (test incident response)
3.7.5 (multifactor)

3.8.4 (CUI marking)
3.8.5 (CUI access)
3.8.7 (removable media)
3.8.8 (portable storage)
3.13.11(FIPS crypto)
3.13.13 (mobile code)
3.14.1 (flaw remediation)
3.14.7 (unauthorized use)

Study Results

The chart below depicts a compilation of compliance summaries from the companies included in our study.

Average percentage of NIST SP 800-171 revision 1 controls implemented


Percentage of NIST SP 800-171 Controls Implemented Across all Clients

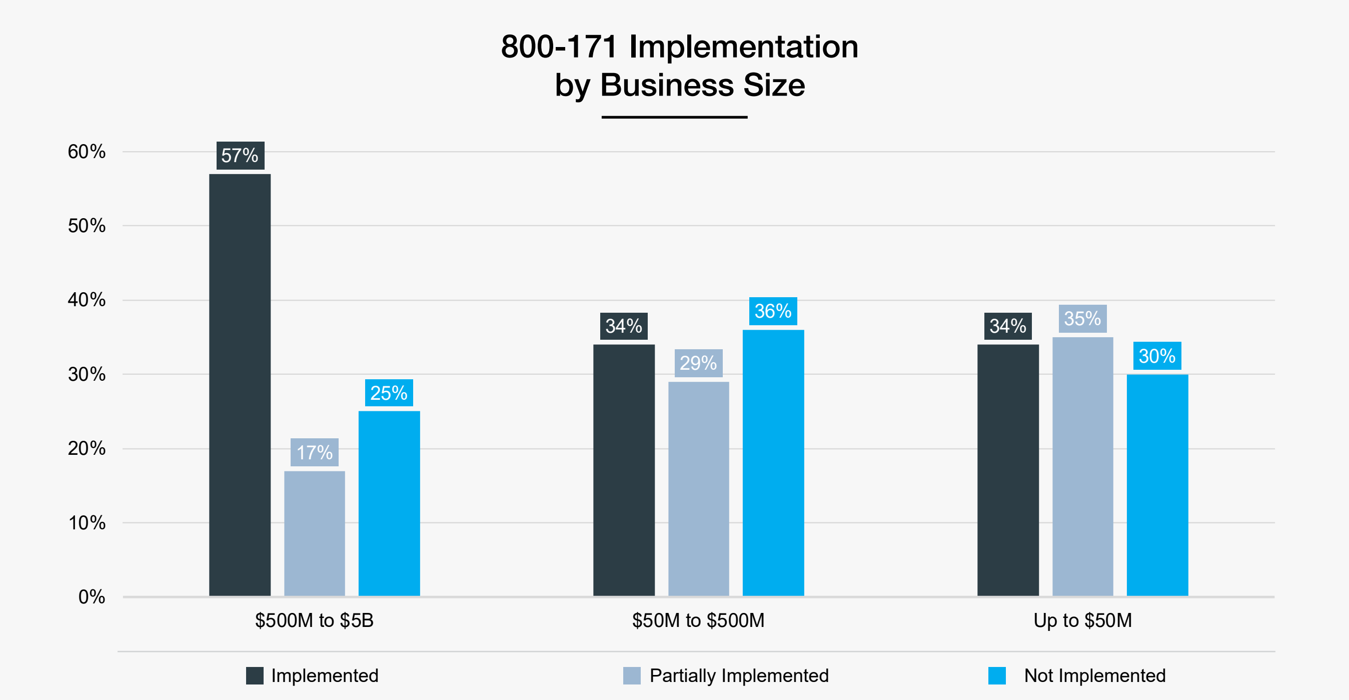
NIST SP 800-171 controls implementation by business size

In general, the larger the company and more robust the security environment, the higher the percentage of 800-171 controls implemented. This was especially evident in those businesses with more than $500M in annual revenue.

Even so, there was statistically little difference in compliance percentages between a $10M firm (annual revenue) and a $100M company. Companies with $5M or less in annual revenue expectedly had the highest percentage of controls not implemented; the highest we discovered was just over 95% not implemented.

Interesting Finding:

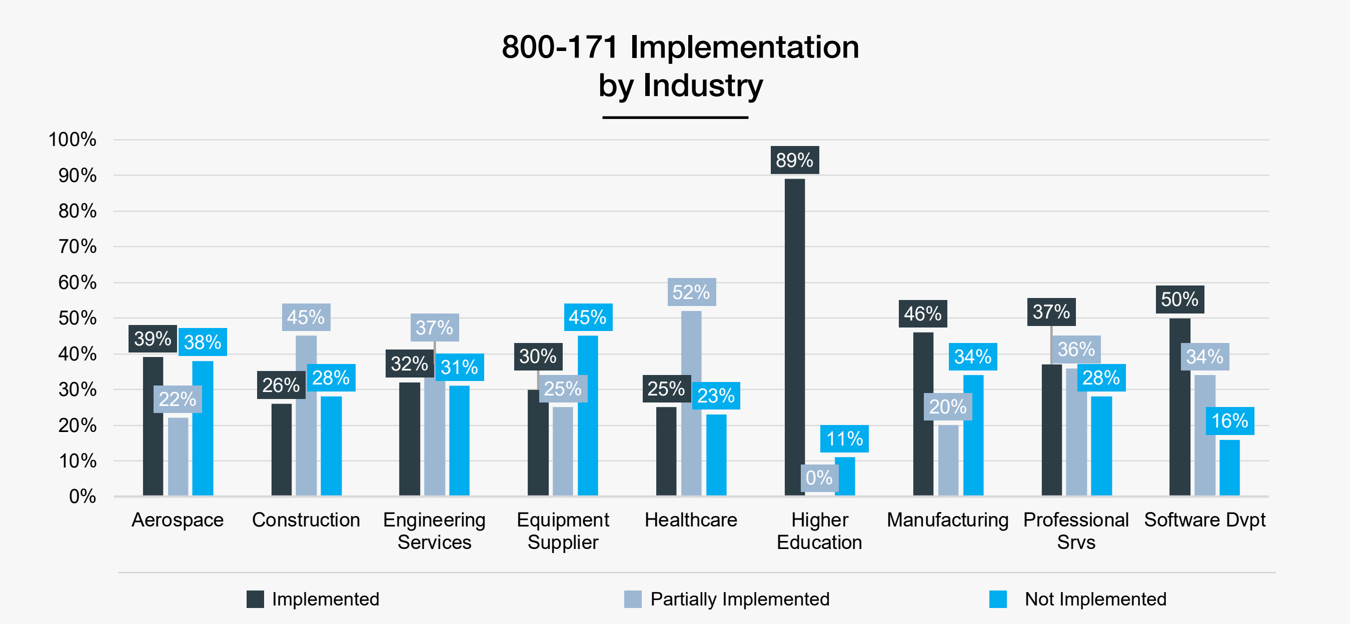
Larger companies with a mature security practice had upwards of 95% of the controls implemented and effective while some smaller companies, or those with less investment in data security, had less than 5% of the controls implemented and effective.



NIST SP 800-171 controls implementation by industry

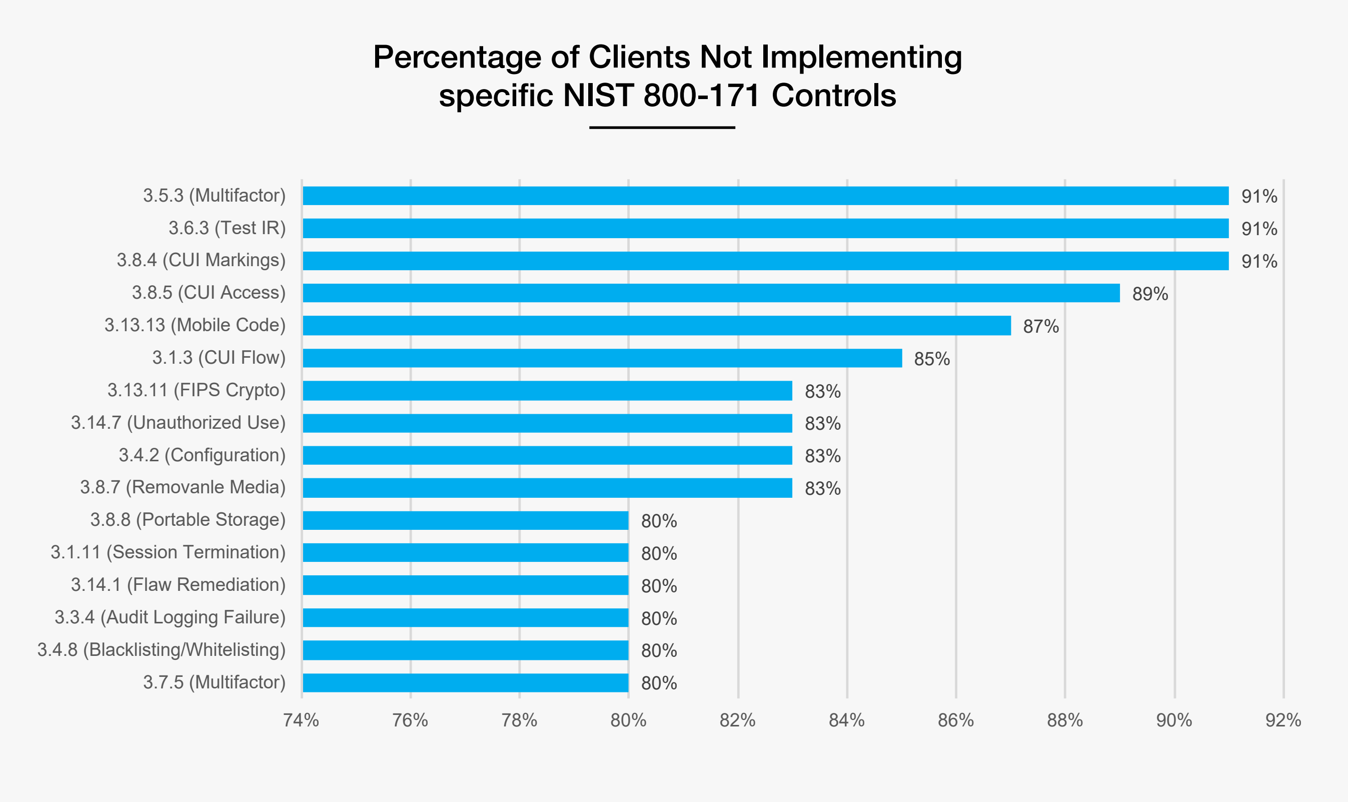
The least compliant defense contractors, on average, were in the following industries: healthcare, construction, and equipment supply (industrial and technical).The most compliant industries, on average, were software development, manufacturing, and aerospace.

Universities were an outlier. As an industry, based on our assessments, institutes of higher learning appeared to be very cognizant of resource allocation towards 800-171 compliance and were subsequently the most secure. Most often, this was because business processes were already segmented, and the environment assessed was used for conducting research and supporting government clients.


800-171 Implementation by Industry

Which NIST SP 800-171 controls were least likely to be implemented?

One significant finding was that 16 specific controls were found to be not implemented by virtually every company we assessed. In the charts below, we have identified controls that were not implemented or found to be deficient at 80% or more of the organizations in this study. These findings were fairly consistent across industries and were found in companies of every size.


Percentage of Clients Not Implementing specific NIST 800-171 Controls

Percentage of Sera-Brynn clients that did not implement the control

91%

NIST SP 800-171 Rev. 1 control 3.5.3: *Use multifactor authentication for local and network access to privileged accounts and for network access to not privileged accounts.*

Root Cause: Organizations are still coming to grips with this requirement.
Note: Multifactor authentication (MFA) has not been well adopted in industry and few clients have fully deployed an MFA solution. This is primarily due to cost, complexity, and ease of use. Many of the commercial solutions available, though not egregious in price, present a level of overhead that some of our clients may not be able to resource immediately. This being said, operating system providers have made significant strides towards enabling MFA for all, which may solve the issue in the near term.

91%

NIST SP 800-171 Rev. 1 control 3.6.3: *Test the organizational incident response capability.*

Root Cause: Businesses have pushed this to the backburner to deal with the technical requirements first.

91%

NIST SP 800-171 Rev. 1 control 3.8.4: *Mark media with necessary CUI markings and distribution limitations.*

Root Cause: Organizations are waiting for better guidance from customers. Based on feedback from customers in the defense spaces, they are not receiving appropriately marked CUI from their government sponsor. As such, they have not been able to determine appropriate marking standards themselves.

89%

NIST SP 800-171 Rev. 1 control 3.8.5: *Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.*

Root Cause: Clients in general had not considered physical movement of media outside of their spaces.

87%

NIST SP 800-171 Rev. 1 control 3.13.13: *Control and monitor the use of mobile code.*

Root Cause: This control has not been well understood by our clients.

85%

NIST SP 800-171 Rev. 1 control 3.1.3: *Control the flow of CUI in accordance with approved authorizations.*

Root Cause: Clients were not clear on the requirements of this control.

83%

NIST SP 800-171 Rev. 1 control 3.13.11: *Employs FIPS-validated cryptography when used to protect the confidentiality of CUI.*

Root Cause: Clients sought to use FIPS “compliant” cryptography vice FIPS-validated and were concerned about resource burdens on information systems.

83%

NIST SP 800-171 Rev. 1 control 3.14.7: *Identify unauthorized use of organizational systems.*

Root Cause: Many clients did not have a method to aggregate appropriate records to detect the activity. Following the guidelines provided in NIST SP 800-137, particularly for Security Incident and Event Management "(SIEM)" would address this control.[++]

83%

NIST SP 800-171 Rev. 1 control 3.4.2: *Establish and enforce security configuration settings for information technology products employed in organizational systems.*

Root Cause: Many clients had established configuration settings but had not fully enforced the configuration baseline or had undocumented variations that indicated a lack of enforcement. A SIEM, as specified in NIST SP 800-137, would help address this control.

83%

NIST SP 800-171 Rev. 1 control 3.8.7: *Control the use of removable media on system components.*

Root Cause: Clients were unsure on how to appropriately do this. Many had not defined removable media and considered it binary, i.e. their only options would be to disable all USB ports.

80%

NIST SP 800-171 Rev. 1 control 3.8.8: *Prohibit the use of portable storage devices when such devices have no identifiable owner.*

Root Cause: As with 3.8.7, clients looked for a technical means to do this and struggled to identify a satisfactory method. Many relied on portable storage to support business processes and had not yet defined an alternative.

80%

NIST SP 800-171 Rev. 1 control 3.1.11: *Terminate (automatically) a user session after a defined condition.*

Root Cause: The only published method to do this is via restricting logon hours which most of our clients do not want to do. In some cases, particularly with research environments, processing functions were running long-term making it difficult to define termination conditions.

80%

NIST SP 800-171 Rev. 1 control 3.14.1: *Identify, report and correct system flaws in a timely manner.*

Root Cause: The failure to implement is due either to legacy systems or lack of vulnerability scanning. Flaw remediation was identified as an issue generally for two separate reasons:

1) Appropriate vulnerability scanning (3.11.2) was not in place and flaws cannot be remediated if a company is not aware of them, which presents a significant risk.

2) Systems beyond end-of-life, e.g. Windows XP/Server 2003, were still in use. This presents an even greater risk.

[++] SIEMs can be costly both in terms of funding and resources and many clients did not have the resources to fund or manage a SIEM. Third-party SIEM management (SIEMaaS) is a more cost effective alternative being considered by many defense contractors.

80%

NIST SP 800-171 Rev. 1 control 3.3.4: *Alert in the event of an audit logging process failure.*

Root Cause: With the typical operating system, there are limited methods to do this without 3rd party monitoring software. Again, a SIEM solution would assist organizations in addressing this control.

80%

NIST SP 800-171 Rev. 1 control 3.4.8: *Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.*

Root Cause: Most of our clients had an ad hoc list of allowed software, but had never specifically defined what is allowed or what is not allowed on their network.

80%

NIST SP 800-171 Rev. 1 control 3.7.5: *Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete***.**

Root Cause: In addition to the issues with MFA identified above, clients were generally not aware of the requirement to terminate the connection.

Larger issues with implementing NIST SP 800-171

Familiarity with the controls. When first reading NIST SP 800-171, certain controls may lead to an assumption, and not until the supplementary information is read, can the control be well understood. 3.13.13 is a prime example; many of our clients read the language "Control and Monitor the Use of Mobile Code" and concluded that this relates to mobile devices. This same reasoning also led to a significant number of clients only applying MFA for remote users. They generally took local to mean "on the LAN", not as it's defined.

Many IT personnel are fully engaged in support of the availability of the network. Seeking to discern meanings from government policies tends to be low on their list of priorities.

Cultural issues. Two significant issues continue to impact security within the defense contracting community.

1) Security is not seen as a profit driver. The resources required to secure a network may cost a company significantly in terms of both time and money.

2) Security requires change. As an example, many businesses have allowed users to maintain local admin privileges on the system and removing those privileges requires a cultural change. That often precipitates significant pushback from the staff. ++

Cloud Services. The movement to cloud services has been encouraged by Sera-Brynn assessors, particularly for clients with a limited infrastructure. There are issues related to this movement.

1) Connecting to the cloud. Many of these cloud services allow for centralized storage of documents in a secure environment. However, there is limited capability to technically restrict access to the cloud environment without increased overhead. For instance, work may be done from the office or anywhere in the world. If the company allows for access outside of its corporate spaces, effective capabilities to prevent non-company owned devices from accessing

++ Removing local admin privileges is not specifically required, but does provide benefits when implementing NIST 800-171.

the cloud environment are minimal. The company could restrict access to corporate IP spaces, but this would necessitate a connection via VPN for remote workers. Newer certificate-based authentication mechanisms may assist in mitigating this issue.

2) Lack of available options. Many cloud services in use are not FedRAMP Moderate baseline compliant. As a 3PAO, we fully support the FedRAMP mandate and suggest additional encouragement of cloud service providers to meet FedRAMP requirements.

Does NIST 800-171 compliance equate to increased security?

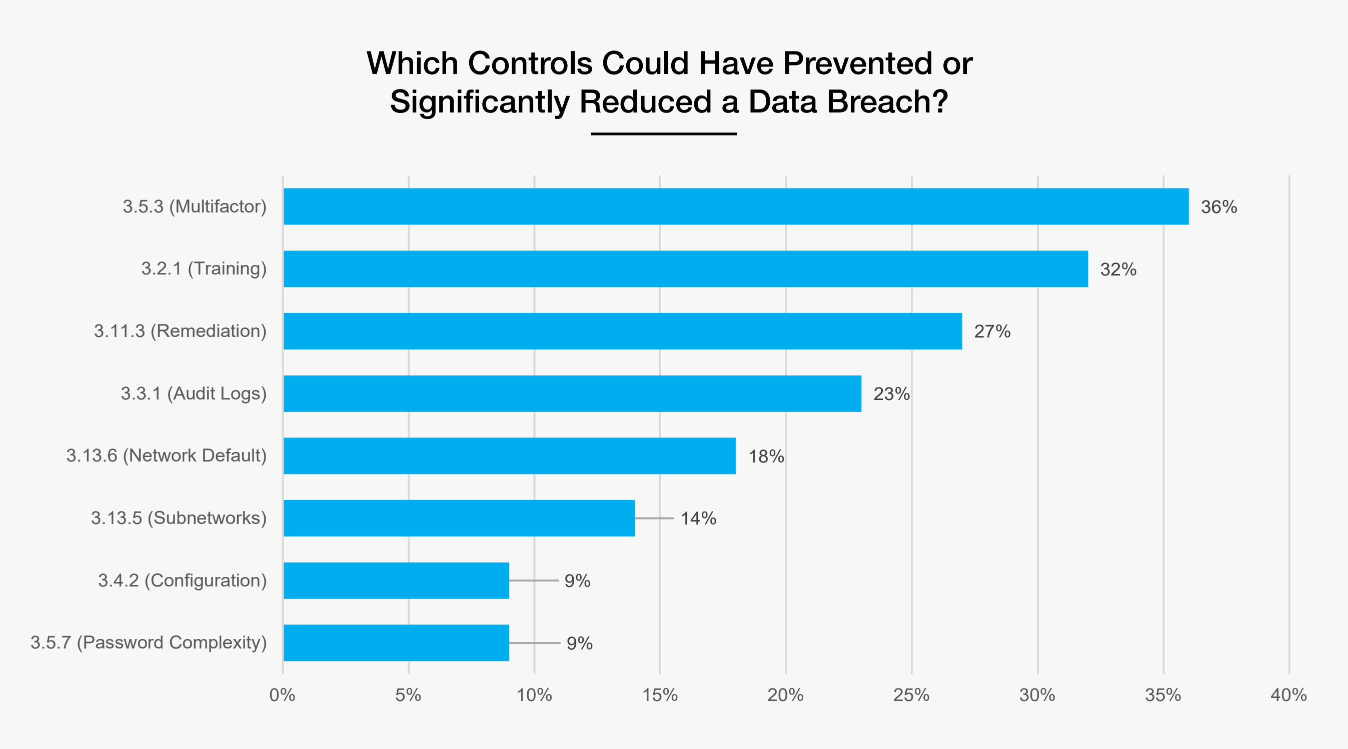
Based on our research, the short answer is yes.

To answer this question, Sera-Brynn reviewed the incident response investigations it conducted within the defense industrial base during the same period of this study. Because the controls specified in NIST 800-171 are directly tied to protecting the confidentiality of an information system, we reviewed recent data breach incidents to determine if implementation of 800-171 controls would have made a difference.

Our findings show that in almost all the incident response cases we investigated, had the 800-171 controls been implemented, a breach most likely would not have occurred, or the impact of the breach would have been significantly reduced. In particular, a lack of MFA (3.5.3), untrained users (3.2.1), and poor patch management (3.11.3) played significant roles in the data breaches we reviewed.

Top Three Controls that could have prevented or significantly reduced ***a third of the data breaches*** *we reviewed:*

3.5.3   Multi-Factor Authentication
3.2.1   Awareness / Training
3.11.3   Vulnerability Remediation



For instance, in approximately 36% of incidents, had MFA been in place, the breach would likely not have occurred. Likewise, had the organization practiced good patch management, nearly 27% of breaches may have been avoided.

While a fully trained and aware user will be a security asset, an untrained user presents a significant vulnerability. More than 30% of breaches Sera-Brynn responded to can be attributed to users that were not aware of the dangers.

Many systems did not have appropriate logging and auditing configured which made conducting post breach investigations difficult and/or incomplete. It also led to delayed notifications of the incident, likely resulting in a more significant compromise.

Methodology

Data set selection

This analysis is based on a sample of companies assessed by Sera-Brynn. Companies ranged from small businesses conducting scientific research to publicly traded companies in manufacturing, consulting, and technology.

Sera-Brynn selected a subset of the companies it has assessed since NIST 800-171 Rev.1 was published in December 2016. Assessments performed prior to Revision 1 were excluded. This is because Revision 1 added additional controls that required development of a System Security Plan and Plan of Action and Milestones; therefore, assessments conducted prior to that time were excluded from the analysis.

Approximately 50 organizations that satisfied the following criteria were selected to form the basis for this study:

- The assessments selected were performed by Sera-Brynn certified auditors and analysts between December 2017 and February 2019.
- The purpose of the assessments was to assess and validate the implementation of NIST SP 800-171 Rev. 1, in its entirety, across a business unit or enterprise.
- The assessments were performed for organizations that were subject to the compliance requirements of DFARS 252.204-7012.
- The assessment locations were geographically dispersed across the United States.
- The assessments were of independent entities with distinct IT environments, as opposed to multiple assessments under the same umbrella organization.
- The survey included both for-profit and non-profit organizations, as well institutions of higher education.
- Small, medium, and large organizations, defined by revenue, were included.

Assessor Qualifications

As a Federal Risk and Authorization Management Program (FedRAMP) Third Party Assessment Organization (3PAO) and Payment Card Industry Qualified Security Assessor (PCI-QSA) company, all Sera-Brynn analysts are required to maintain industry standard certifications and conduct assessments in accordance with 3PAO standards.

Assessment Methods and Reference Tools

The work performed by Sera-Brynn that formed the basis of this study was assessments against the NIST 800-171 controls. Assessments typically started with data discovery to include technical scans, policy review, personnel interviews, and other inputs. Each control was then validated in order to determine the effectiveness of its implementation. Each of the 110 controls was graded as Implemented, Partially Implemented, or Not Implemented. A Plan of Action and Milestones (POA&M) was developed. The NIST 800-171 assessments were conducted in full cooperation with the clients. Throughout the engagement, the assessors advised decisionmakers on remediation issues based on organizational considerations, risk tolerance, and resource availability.

The primary guide for our security assessments is NIST SP 800-171 revision 1, “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.” 800-171 has gone through multiple updates since its release and all have helped clarify and provide additional guidance with regards to the controls.

NIST SP 800-171 implementation requires an organization to determine the intent of the control and the level of risk behind various implementation strategies. Over the course of an assessment, Sera-Brynn analysts refer to supplemental guidance in NIST SP 800-53 Rev. 4 and review NIST SP 800-171A, “Assessing Security Requirements for Controlled Unclassified Information (CUI)” when determining if the implementation is acceptable.

Other reference documents include the NIST Handbook 162, “NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements” and the DoD-provided “Frequently Asked Questions (FAQs) regarding the implementation of DFARS Subpart 204.73 and PGI Subpart 204.73, DFARS Subpart 239.76 and PGI Subpart 239.76, FAQ REVISION.”

In some cases, our assessors may contact the DoD Chief Information Officer (CIO) directly to request clarification.

Conclusion

NIST 800-171 is a solid cybersecurity baseline for organizations handling sensitive information. However, it has not been well implemented even when required.

Each of our clients has been unique, not only in business type and size, but internal capabilities and leadership support for secure information systems operations. Most often, the IT staff welcomed our findings as they were in agreement with what they already suspected. The security issues rise from the lack of resources (funding/personnel) given to remediate the problems. The DFARS regulation has given IT departments more ammunition to argue for additional security measures within their respective companies, but based on our findings, this has not fully percolated through the Defense Industrial Base.

IN CONCLUSION:

1.The majority of defense contractors are not fully DFARS 252.204-7012 compliant.
2.There is no cookie-cutter approach to compliance…every business is different.
3.The quickest way to “check” the supply chain is to review, validate (and remediate) SSPs.

The DoD has called for structured auditing of controls to begin in 2020.[2] In the meantime, the DoD, in conjunction with its large prime contractors, should ensure that all companies are aware of the requirements and understand the cybersecurity controls of NIST 800-171. The Undersecretary of Defense for Acquisition and Sustainment has directed the Defense Contract Management Agency (DCMA) to begin reviewing prime contractor procedures to assess compliance of their Tier 1 Level Suppliers with DFARS Clause 252.204-7012 and NIST SP 800-171.[3] Based on our experience of conducting 800-171 assessments, **self-attestations or yes/no surveys are not sufficient to determine compliance with the regulation.**

We do believe a high-level, but impactful assessment of compliance could be effectively done today through a review of System Security Plans (SSPs). Requiring SSPs to be audited would almost certainly ensure that the organization is aware of the 800-171 control requirements.

For additional information on Sera-Brynn's Cybersecurity Audit and Advisory services, to include DFARS 252.204-7012 assistance, please visit our website (Sera-Brynn.com) or contact us directly at (757) 243-1257.

[2] https://federalnewsnetwork.com/defense/2019/03/dod-to-start-crackdown-on-contractors-not-complying-with-cybersecurity-standards-will-also-add-more-compliance-rules/
[3] https://www.acq.osd.mil/dpap/pdi/cyber/docs/USA000140-19%20TAB%20A%20USD(AS)%20Signed%20Memo.pdf

SERABRYNN

GLOBAL LEADER IN CYBERSECURITY COMPLIANCE