A cost-benefit approach to optimizing security precaution adoption

Noa Barnir, Neil Gandal, Tyler Moore, and Vincent Scott

Forthcoming, 2025, Information and Computer Security

University of Tulsa, Tel Aviv University, and Defense Cybersecurity Group

August 2025

Abstract

Purpose: All U.S defense contractors were required to have fully implemented the 110 security requirements included in NIST Special Publication 800-171 entitled "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" by 1 January 2018 whenever a system owned, or operated by or for, a contractor processes, stores, or transmits controlled unclassified information (CUI). Despite the mandate, adoption has been minimal, mostly because the requirement is so costly and time-consuming that medium and small firms cannot afford to comply. Since the adoption of security precautions is costly and time-consuming, in this paper, we propose a constrained optimization methodology to examine this issue.

Design and Methodology: In this paper, we introduce a method to significantly reduce the number of required precautions by soliciting expert opinion as to the perceived benefits and costs of all precautions. We defined the difference between benefits and costs as value.

Findings: In the key constrained optimization exercise we conduct, we show that including only the top 50 security precautions (out of the 110 security precautions) led to just a very small decline in value.

Originality: This paper makes an important contribution to information security research. To the best of our knowledge, no one has conducted similar analysis on the 110 proposed precautions.

Keywords: Security precautions, cost-benefit analysis, defense contractors, constrained optimization, robustness analysis

Acknowledgement: Gandal and Moore gratefully acknowledge support from the US National Science Foundation (NSF) Award No. 2147505 and Award No. 2452738 and the US Israel Binational Science Foundation (BSF) Award No. 2021711. We are grateful to the editor and two referees whose comments and suggestions significantly improved the manuscript.

1 Introduction

During the "Promoting Competition in AI" conference[1], former US National Security Advisor and Secretary of State Condoleeza Rice was asked "how you think the US government is doing today with respect to being able to leverage the commercial sector to acquire the technologies that are clearly going to be needed for national security purposes…". She replied[2] "I think we're doing very poorly. Very poorly. And it's largely because the procurement and acquisition processes in the defense department are baroque to say the least." She goes on to note that it is virtually impossible for small companies with great ideas or products to "penetrate the Pentagon".

Why might Secretary Rice take such a dim view of US competitiveness caused by procurement challenges? There are undoubtedly many factors at play, but one area of increasing concern is the heavy burden being placed on defense contractors of all sizes to secure their operations and computing infrastructure. All U.S defense contractors were required to have fully implemented the 110 precautions of 800-171 by 1 January 2018 whenever a system owned, or operated by or for, a contractor processes, stores, or transmits CUI[3].

However, a number of significant challenges continue to exist. Adoption has been minimal[4], primarily through a combination of factors including high cost of implementation and poor cyber prioritization based on perceived risk in businesses and

[1] See https://siepr.stanford.edu/events/promoting-competition-ai.
[2] The question and answer are extracted from the transcript of the conference.
[3] Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting, https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012
[4] DoD Inspector General Audit Report, "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems," July 23, 2019. https://media.defense.gov/2019/Jul/25/2002162331/-1/-1/1/DODIG-2019-105.PDF

other organizations. The high cost of implementation represents a significant challenge for the U.S. in attempting to protect the sensitive but unclassified information in their military supply chains, while also meeting other strategic imperatives including expanding participation by those that offer significant innovation and cost advantages (OSD 2023).

Despite this, the US Department of Defense (DoD) has mandated full implementation of all controls, including for small and medium sized businesses which in 2023 received 25% of prime contracts from the US DoD[5]. Waivers granted by DIB organizations require explicit written approval by the DoD's Chief Information Officer (CIO). The DoD CIO's office has indicated that very few waivers will be granted.

Indeed, although a few such waivers are theoretically possible, we are unaware of any instance where the DoD CIO has granted any waiver. This is part of the implementation challenge that we seek to address. Full implementation of controls, and the enforcement of all controls through an expansive and detailed audit process, may not be a productive use of scarce cybersecurity and IT resources.

Since the adoption of security precautions is costly and time-consuming, in this paper, we propose a constrained optimization methodology to examine this issue. Our method aims to rationally reduce the number of required controls in order to reduce cost and lower the burden of implementation while maintaining those precautions that offer the greatest value, which is the difference between "benefit" and cost.

[5] See https://www.defense.gov/News/News-Stories/Article/Article/3339784/dod-increases-efforts-to-bring-small-businesses-into-defense-industrial-base/

In particular, we survey six cybersecurity experts and have them rank the "benefit" from and "cost" of proposed security precautions. The six cybersecurity experts were chosen because of their cybersecurity experience in the Defense Industrial Base, implementing, consulting, assessing, and leading cybersecurity programs based around the NIST SP 800-171 security requirements framework.

All participants are recognized, published professionals in the US Federal Government cybersecurity and compliance ecosystem. Each has more than 10 years of experience in cybersecurity and compliance, and each has been responsible for both implementing secure and compliant systems, and evaluating security and compliance in other organizations. This provides the respondents with good insights on the cost, and effectiveness of controls from both an implementation and compliance assessment perspective. The evaluation of these 110 security precautions took approximately four hours per participant, which is a lot of time for someone participating in a survey, especially such highly skilled individuals, with high opportunity costs.

In our setting, the six security experts ranked the "benefit" and "cost" of all 110 precautions across 14 categories documented in NIST Special Publication 800-171 entitled "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations". The difference between the "benefit" and "cost" of all 110 precautions is denoted as "value". Importantly, there is a very high correlation between the DoD benefit rating and the average of the experts' benefit rating for these 110 security precautions. Additionally, there is also a high correlation among the expert's estimation of the cost of these 110 security precautions. (The DoD did not estimate the costs of these 110 security

precautions.) Further, the correlation among the experts' ratings gives us evidence of the reliability of our rankings and estimates of benefit, cost, and value.

Our analysis shows that it is possible to significantly reduce the number of precautions without sacrificing significant value. In our key constrained optimization exercise, we choose the best 50 precautions (ranked by value). When keeping the best 50 precautions, the total value decreases by only sixteen percent when compared to the case with all 110 precautions. In this way, we eliminate fifty-five percent of the precautions without sacrificing much value.

We also conducted extensive robustness analysis and showed that our results are virtually unchanged when we use different combinations of experts. This stems from the large positive correlation of the rankings by the experts. This provides confidence that our results are robust even with the small sample size. It also gives us confidence that adding more experts to the analysis would not change our results.

We also, however, recognize that this is a proof-of-concept paper – and we do not expect the DoD to immediately rush to implement our exact findings. Rather, we hope that our analysis will stimulate a conversation about how to move forward, since small and medium defense contractors cannot afford to comply with the current certification process that involves all of the 110 security precautions.

2 Background and Motivation

Over the course of the last 20 years, the US Government (USG) and the Department of Defense (DoD) have been advancing their approach to cybersecurity both for their internal networks and their supply chains. In 2010 President Obama signed an executive

order, EO 13556 Controlled Unclassified Information (CUI), to establish an open and uniform program for managing information across the USG that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies. In that same year the USG adopted the DoD's Benefit Management Framework (RMF) as the backbone of its approach to cybersecurity for information that required protection that would become defined as CUI under the new executive order.

In 2014 the DoD began the process with the National Institute of Standards and Technology (NIST) of tailoring the RMF controls to provide a focused standard for the Defense Industrial Base around securing the confidentiality of the DoD's sensitive information, principally as codified in the new CUI program. This resulted in the creation of NIST Special Publication 800-171. These precautions, or security requirements as they are termed in the publication, provide what the DoD considers to be the minimum set of security requirements for their sensitive information. See the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting"[6].

As noted, the precautions have not been broadly implemented across the Defense Industrial Base (OIG 2022). In November 2022, CyberSheath in conjunction with Merrill Research published a report stating that only around half of the Defense contractors had submitted a cybersecurity score indicating their level of implementation for the required precautions. Of those who had submitted, the average level of implementation was 30%, far less than the 100% implementation that has been required since 2018. This is far from the first such indication, however. The Defense Inspector

[6] https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012

General's Office has issued a series of reports over the last 5 years indicating that significant gaps existed in cybersecurity precautions implementation across the DIB and inside the DoD as well (OIG 2019).

As a result of these gaps, the DoD has undertaken an effort to develop the Cybersecurity Maturity Model Certification (CMMC) as a mechanism for certifying DIB contractors as complying with these security contractual requirements. Established in 2020 the DoD has stated their intent to fully implement the certification requirement in all contracts starting 1 October 2025. We believe that we can contribute to this process by making implementation much more feasible without significantly sacrificing security.

Certification requirements in contracts for various standards are not new. AS9100 Quality Management System – Requirements for Aviation, Space and Defense Organizations for example has been in use in various forms since 1999. CMMC however and its requirement for full implementation of all precautions with little to no options for alternative but equally effective precautions in the highly complex and varied environment of DIB contractor networks presents significant challenges.

The challenge of 100% perfect implementation without variation is not unique to the DIB. At the direction of Congress, the Government Accountability Office (GAO) studied the DoD's implementation of the 800-171 precautions, a subset of their existing requirements and found that they were 70-79% implemented (US GAO 2022). Far better than 30% but still a sizable gap from a 100% implementation with no feasible allowance for alternative precautions or benefit management in their application.

In the creation of the original 800-171 set of precautions NIST looked at the precautions that existed in the current government regulations for protecting the

confidentiality of information and how they could be applied to contractor networks. They did not consider the potential benefits and costs of implementing those precautions. Simply put, they did not consider bang for the buck. Some provide significant value (i.e., benefit less cost.). Implementation of two factor authentication (2FA) is likely be an example of a precaution that has a large benefit relative to its costs. But, as one would expect, not all precautions are created equal and some have costs that outweigh the benefits.

The DIB is a broad and diverse set of organizations and many of its smallest members are providing the innovation and adaptability needed to meet our greatest challenges. The implementation of a one size fits all set of precautions *designed initially for implementation by large government organizations* is likely to cause significant challenges for the USG and the contractors that seek to support them. By focusing on a more limited set of high value precautions, the USG can achieve a similar benefit impact with far less cost and attrition in its supply chain.

We believe that a greater focus on compliance and certification of the most valuable precautions will provide the best approach for the Department in pursuing its cybersecurity goals. 100% perfect implementation is likely not achievable. We illustrate the benefits of our methodology below.

3 Literature

We now briefly survey the relevant literature. For an excellent overview of the development of the information security culture between 2000 and 2013, see Karlsson et al (2015). Additionally, Schinagl and Shahim (2020) provide a nice overview of

information security governance. For a comprehensive theoretical discussion of security precautions, see Woods and Boehme (2021). Moore et al (2016) found that firms often simply adopt frameworks of one kind (e.g., the NIST Cybersecurity Framework, COBIT, SANS Critical Controls). The problem is that these frameworks do not explicitly evaluate how taking precautions affects the security level of their organization, and ultimately whether those precautions make a breach less likely to occur.

Using survey data from Israeli firms about their cyber defenses, Gandal *et al*., (2023) estimate the relationship between security precautions potentially undertaken by enterprises and the likelihood of experiencing a cyber-incident. They find that increased adoption of several basic security precautions significantly reduces the likelihood of being breached.

A few other studies have also investigated the relationship between security precautions potentially undertaken by enterprises and the likelihood of experiencing a cyber-incident. For example, Li *et al*. (2023) examines reports of IT investment at 311 publicly-traded US firms and compare it to publicly disclosed data breaches at those firms. It constructs a proxy for firm cybersecurity awareness by examining regulatory filings with the SEC (10-K reports).

Quite a few researchers have focused on cybersecurity investment in the US healthcare sector. This is because detailed data on hospital attributes are readily available, and the HITECH law has required public disclosure of data breaches involving private health information since 2010. See Gandal *et al* (2023) for discussion of these papers.

A few researchers have investigated the impact of these guidelines on the defense industrial base. Sundarajan et. al (2022) assessed 127 defense contractors and identified

the most common deficiencies. Their findings underscore the difficulty firms of all sizes are facing in satisfying all requirements. Imsand et al. (2020) surveyed small businesses intending to comply with NIST 800-171 requirements about their cyber security practices. They found that these small businesses tend to adopt poor operational security practices.

These findings are consistent with other studies of small businesses seeking to implement different frameworks such as the NIST Cybersecurity Framework (Chidukwani et al. 2022). Yair and Gafni (2022) highlight the difficulties small businesses face in order to achieve CMMC certification. They propose a framework to quantify the technology footprint required to achieve successful certification to lower the burden of self-assessment. In a follow-up study, they evaluated this footprint index by surveying subject matter experts (Gafni and Levy 2023). This approach nicely complements the work presented here. Whereas Gafni and Levi use expert ratings to evaluate how controls should be counted in the index, we survey experts to identify the most cost-effective precautions.

While there has been some work on optimizing the selection of cybersecurity controls, it has thus far not focused on the decision-making of smaller enterprises. Almeida and Respicio (2018) construct a decision-support model that uses integer programming to select a set of security controls that maximize coverage while minimizing expected costs. Yevseyeva et al. (2015) use portfolio optimization models to select subsets of security controls. Kiesling et al. (2016) construct an agent-based model to capture threat actor and defender behavior in a manner that optimizes control selection.

The history of how the US Government handles unclassified information and why the CMMC was developed is described in Strohmier et al (2022). The cost of implementing extensive governmental control frameworks has also been pointed out. Gonzales et al (2020) emphasized the cost of advanced cybersecurity capabilities for small and medium sized defense firms. They proposed some provision of these tools for the Defense Industrial Base; however, they did not examine the possibility of optimizing the application of these controls in order to reduce cost while still providing significant risk reduction.

Each of these papers construct a more complex mathematical model than we devised. The advantage of our simpler approach is that we grounded it with expert judgement to identify the optimal subset of controls, which yields actional recommendations for the specific case of NIST 800-171 and CMMC. By contrast, the aforementioned models constructed elaborate optimization frameworks but did not seed them with realistic data.

Brotby and Hinson (2016) provide a comprehensive review of the construction and use of metrics in the evaluation of security programs. In particular, there have been developments in financial metrics, for example, Gordon & Loeb (2006) show how to optimize the value of information security through cost-benefit analysis, using standard accounting methods. Johnson (2019) focused on general approaches to assessment for various frameworks, including a discussion of various assessment approaches. None of these papers specifically address compliance/cybersecurity management challenges for small and medium enterprises.

4 Methodology

We use a cost-benefit framework for our analysis in this paper. Cost-benefit analysis is a well-established empirical methodology. Many researchers believe that cost-benefit analysis was first applied in the US in the 1930s. Others argue that cost-benefit analysis emerged much earlier (in the early to mid-1800s.) Regardless of when it was first employed, cost-benefit analysis is regularly employed in many disciplines – and it is a well-accepted method to decide (for example) whether a government should undertake an infrastructure project or which is the best alternative to choose among several possibilities.

In particular, constrained optimization is the methodology we apply in the paper. Constrained optimization is widely used in both academic research and practical applications. Simply put, it optimizes subject to well defined constraints. (See section five for details.)

This methodology is common in various sectors, including transportation, logistics, healthcare, and financial risk management. Specifically, in cybersecurity, constrained optimization provides a structured approach to effectively allocate limited resources while ensuring robust protective measures. This makes it particularly suitable for the defense sector, which often deals with resource limitations. Our goal in this empirical analysis is to demonstrate that it is feasible to greatly reduce the number of security precautions without sacrificing much value.

We conducted an analysis of the 110 precautions of 800-171 by using expert ratings both of benefit and cost in order to identify what are the most *valuable*

precautions. We surveyed six cybersecurity experts who are experts in the field and particularly knowledgeable about the precautions and 800-171.

Table I presents the background of our experts; in addition to their extensive experience, all the respondents are deeply involved in the CMMC assessment ecosystem, most as both assessors and implementers. CMMC as an assessment standard was only 3 years old at the time of collection and all respondents have been involved since its inception. One of the respondents holds a PhD in Cybersecurity and 5 hold master's degrees in information systems or related fields. The reviewers come from different industries.

In any case, the principles of cyber security are universal across industries because everyone is using the same software. All respondents are extremely familiar with the controls they were asked to assess with direct knowledge of requirements to implement those controls and good understanding of the cybersecurity benefits. All selected experts have extensive experience in defense industrial cyber security. There is a very limited knowledge pool of such experts. That is, there are very few people in the world who have the expertise to undertake this work.

Such experts are very busy and there is a large demand for their expertise. We are fortunate that these experts agreed to do this without charging us. Given the time involved, and the typical consulting fees of such experts, we likely would have had to pay upwards of $1500 per expert to do this work! In summary, these people have extensive experience in the field.

The experts then ranked the “benefit from” and the “cost of” of all 110 precautions across 14 categories. The benefit rankings were from 1-5, with “5” indicating a “very large contribution/benefit”. On the other hand, “1” represents a “small to negligible contribution/benefit”. The six experts used 1,2,3,4, or 5 as responses. The DoD also rated the benefit on a 1-5 basis, using 1, 3, or 5 as responses. Formally, “5” was defined as a “very large contribution to risk reduction”, while “1” represents a “small to negligible contribution to risk reduction”.

Clearly risk reduction is the benefit from precautions. We use “benefit” rather than “risk reduction” for ease of presentation and because this terminology is consistent with economic analysis.

Regarding the 1-5 scale, we employ that because the DoD used it when ranking the benefits of each of the 110 precautions and we wanted to compare the DoD ranking of the benefits of the 110 precautions with those of our experts. It was important in particular to examine whether there was a high correlation between the DOD benefit rating and the average of the experts' benefit rating.

The experts were given a predefined explanation of what constitutes a "1" versus a "5” for both benefits and costs. In the case of the benefits, the explanations are as follows:

5	Very large contribution to risk reduction
4	Large contribution to risk reduction
3	Moderate contribution to risk reduction
2	Modest contribution to risk reduction
1	Small to negligible contribution to risk reduction

In the case of the costs, the explanations are as follows:

5	Very difficult to implement/Very expensive
4	Difficult to implement/expensive
3	Moderate cost and difficulty
2	Modest cost and difficulty
1	Small or negligible effort to implement

Encouragingly, there is a very high correlation between the DoD benefit rating and the average of the experts' benefit rating. We calculated the means by eliminating the highest and lowest value, so the means were calculated using the four middle rankings. The correlation between the DoD benefit measure and the average benefit of the experts is roughly 0.48. As a result we can confidently proceed with the analysis.

In the case of cost, as noted above, the rankings are also from 1-5, with "5" for precautions that are "very difficult to implement and/or very expensive". On the other hand, a ranking of "1" is for precautions that require "small or negligible effort to implement". Again, the experts used 1,2,3,4, or 5 as responses. The DoD did not "estimate" the cost of implementing the precautions.

We then computed "value" as the difference between benefit from and cost for each of the six experts regarding all 110 precautions. That is value = benefit – cost. For the analysis, we eliminated the maximum and minimum values for each precaution for each of the three measures. We then calculated the means for each of the three variables.

5. Analysis and Results

There are fourteen categories of precautions. They are:

- Audit and Accountability
- System and Information Integrity
- Media Protection
- Identification and Authentication
- Personnel Security
- System and Comm. Protections
- Access
- Awareness and Training
- Risk Assessment
- Maintenance
- Physical Protection
- Security Assessment
- Incident Response
- Configuration Management

Most of the categories are self-explainable; however, a full explanation of each can be found in NIST 800-171.

Summary Statistics by Category are shown in Table II in the Appendix. Table II shows that there is a huge difference among the categories in terms of benefit, cost, and value. Of particular interest is the average value of precautions with positive value in each category. (Table II is sorted by that measure.)

Constrained Optimizations: We performed several constrained optimization exercises, where we minimize the number of precautions subject to certain criteria. See Table III in the Appendix for benefit, cost, and value for each of the constrained optimizations.

- One obvious and simple exercise is to include only precautions with mean values greater than zero. This exercise only eliminates 23 precautions. Hence, it is not useful in practice if the goal is to significantly reduce the burden of certification.
- The second exercise is to include precautions with the following two constraints (i) positive mean values and (ii) benefits exceeding 2.5. The idea here is that in addition to including precautions with high values, we might want to include precautions with high benefits even if the associated cost is high as well. This exercise eliminates 34 precautions. Interestingly, the total value almost does not change, relative to the case when we include all 110 precautions. The total value is 86 with all 110 precautions included, while it is 85 without the excluded 34 precautions. The average value per precaution without the 34 precautions increases significantly relative to the case when we include all 110 precautions (1.12 vs. 0.78).
- The third exercise, which we believe is the most important and revealing, was to constrain or limit the number of precautions. Here the constraint was to include only the top 50 precautions in terms of value. By definition, this exercise eliminates 60 precautions or 55 percent of the 110 precautions. The total value falls only slightly, relative to the case when we include all 110 precautions (72 vs. 86), which is a decline of 16 percent. On the other hand, the average value per precaution increases dramatically relative to the case when we include all 110

precautions (1.44 vs. 0.78). This represents an 85 percent increase in the average value per precaution relative to the case when we include all 110 precautions. The category "Security Assessment" which has only four precautions does not have a precaution in the top-50.

- Exercises 4 and 5 are slight moderations of exercise 3, and result in virtually identical results as in exercise 3. In exercise 4, we add an additional constraint so that at least one precaution from each of the fourteen categories is included in the top 50, and Table III shows that this did not change the total value associated with this exercise. In exercise 5 we compute the top-50 precautions with the highest value subject to the constraint that at least 25 percent of the precautions in each category are included. Again, the results are virtually identical to exercise 3.
- In exercise 6, we include only precautions with a mean benefit of 5. There are only 44 such precautions. Here, strikingly, the average value per precaution is very low and it is virtually identical to the case when all 110 precautions are included. This shows that only looking at benefits and ignoring costs is not a sensible thing to do.

Exercise three in particular illustrates the power of the methodology. The elimination of sixty precautions in exercise three is associated with a small fall in total value and a large increase in average value per precaution. That is by reducing the precautions by more than 50%, we only slightly reduce the total value while we dramatically increase the value per precaution.

The loss of value is minimal when we select only the top 50 security precautions (out of the 110 security precautions) because some precautions have a "negative" value

or a value of zero. In the case of precautions with a negative value, the estimated cost is greater than the estimated benefit. For example, if the benefit of a precaution is "2" out of five, where five is the highest benefit, and the cost of the precaution is "3" out of five, where five is the highest cost, then the value of that precaution, which is the benefit minus the cost, is actually negative (2-3=-1)

Table IV in the Appendix shows the top-50 precautions by category. It suggests that there is a large difference among the various categories in terms of importance.

- The most important categories in terms of the most precautions in the top-50 are "Access Control", "Identification and Authentication", "System and Information Integrity", and "System and Communications Protections". All four of these categories have at least five precautions in the top-50 and at least 50 percent of their precautions are included in the top-50.
- Two additional categories have three or less precautions, but all of their precautions are in the top-50.
- None of the other eight categories have more than 33% of their precautions in the top-50. This suggests that these categories are probably less important than the other six categories.

6 Robustness Analysis

Table V in the Appendix shows our key constrained optimization exercise (exercise #3), where we selected the top 50 security precautions using all six experts. In the exercise, we eliminated the highest and lowest values for benefit and cost for each precaution. The question is whether our results are robust to using different combinations of experts.

In Table V, we present seven different robustness scenarios. In the first six scenarios (denoted "Options 1-6" in the Table), we eliminated one of the experts and repeated the exercise using the remaining five experts. Since there were six experts, we have six such robustness exercises. In the seventh robustness exercise (denoted "All Six Experts" in the Table), we included all six experts, but we did not eliminate the highest and lowest values for benefit and cost for each precaution.

Table V in the appendix shows that all of the results are very similar. In the original constrained optimization, we had a value of 72 when we kept only the top 50 security precautions by value. All of the results for the seven robustness exercises fit into a very tight interval for value, from 66.4 to 74.8. The mean value of the seven exercises in 71.6 – and the variance is low.

In terms of how many of the precautions are included in the same top 50 security precautions as Exercise 3, Table V shows that the numbers range from 41 to 44, also a very tight range with low variance. It also shows that we can be fairly confident that we have chosen (at least) the 41 top precautions! We believe that is quite impressive. Thus our results seem quite robust.[7]

Since we wanted to compare the experts' evaluations with those of the DoD, it made sense to use the 5 point scale, that is this way we compare "apples" with "apples". Hence, we applied the same 1-5 scale. It is important to point out that, given the high correlation between experts' evaluations, the results would have been qualitatively similar with 3,5,7, or 10 point scales. We now illustrate this using a three-point scale.

[7] The description of the top 50 precautions from our most important exercise (#3) appears in Table VI in the Appendix. The 34 precautions eliminated by exercise two appear in Table VII in the Appendix.

In order to illustrate that our results are qualitatively similar with a different scale, we re-calibrated our scale to a three-point scale as follows:

Rankings of 1 or 2 were converted to “1”

A ranking of 3 was converted to "2”

Rankings of 4 or 5 were converted to “3”

We then repeated the analysis regarding our most important exercise (exercise 3) where we kept the top 50 precautions. Our results are virtually the same: with the three-point scale, when we only include the top fifty precautions, the value (relative to including all 110 precautions) declines by only 14% vs. a decline of only 16% percent using the five-point scale. This shows that our results are robust to different scales.

These important results obtain because of the relatively high correlations among the experts’ evaluations of the benefits and costs of all of the constraints. The high correlation among rankings means that our results would not qualitatively change if we added additional experts.

The results, of course, also show the limitations of our analysis, since there is some difference in the top 50 precautions. This is why our paper is essentially a proof of concept. We hope that the DOD will find the exercise to be quite interesting as a way forward, since small and medium contractors cannot afford to implement all 110

precautions. With their very large budgets and resources, they could include a larger number of experts and conduct a bigger survey.

7 Implications and Concluding Remarks

Requiring all defense contractors, regardless of size or sophistication, to comprehensively implement a complex set of 110 security precautions is not realistic, especially for small and medium firms. This paper sets out a principled approach to identify a subset of these precautions that could be adopted to provide maximum security benefit at significantly reduced cost. In particular, we showed that eliminating more than half of the precautions can be accomplished without sacrificing much value.

The approach presented here is very straightforward to implement. We primarily view this as a proof-of-concept. A limitation of our work was that we only included six experts and used a simple 1 to 5 rating of the benefits and costs. In future work, it would be ideal to include more experts and finer distinctions among the ratings, perhaps a 1 to 10 scale rather than a 1 to 5 scale. Nevertheless, given the relatively high correlation among the experts' assessments of the benefit and cost of the 110 precautions and the key results of the constrained optimizations we conducted in exercise three and the robustness analysis we conducted, we believe that our results would be essentially the same.

This research is valuable to the US Department of Defense and its Defense Industrial Base in terms of potentially alternative approaches to assessment and enforcement that offer opportunities for streamlined enforcement. It also applies to all contractors for the US Federal government as this same standard underlies the protection of US Controlled Unclassified Information. The US Department of Education for

example has publically indicated their intent to mandate the implementation of NIST 800-171 requirements on US Student Aid information. This would represent a large expansion. A number of departments, including NASA, the Department of Energy, and GSA all have various regulatory changes in process to roll out mandatory implementation of the standard. This paper offers a novel approach to effective enforcement.

This approach could also be applied to other frameworks and standards in order to maximize return on investment in terms of real security and risk reduction by focused limited implementation and enforcement efforts on those security requirements that have the greatest impact.

Although the DoD recently published a new draft CMMC rule, the draft is linked explicitly to the current version that we examined. In any case, we believe that our methodology can easily be employed in this case as well and the most important precautions and categories will remain the ones we identify in this paper. Indeed, we expect that our results will be essentially the same.

A number of other cybersecurity frameworks exist for businesses; the NIST SP 800-171 framework, however, has unique regulatory application to the handling of US Government (USG) information defined as controlled but unclassified information. The USG has long maintained a classification system that is a model for most global governments. Originally established in March of 1940 by then President Franklin Roosevelt, it outlined basic classifications of information surrounding military equipment and operations. Refined during World War II and the Cold War, it continues to lay out the requirements for “classified” information. Since 9-11 the USG has been focusing

additional efforts around securing controlled but unclassified information that it considers sensitive. NIST SP 800-171 is a standard for civilian systems that process, store, or transmit controlled unclassified information (CUI) based on the Moderate confidentiality controls contained in the overarching government framework for cybersecurity, the Risk Management Framework (RMF). Thus NIST SP 800-171 security requirements are derived from RMF controls focused solely on confidentiality and leaving out controls focused on integrity and availability. In this, it departs from other standard commercial frameworks such as 27001, COBIT, and the FAIR model. All of these models present an approach to understanding and dealing with risk to organizations' information. Under the NIST SP 800-171 model, the USG has already made risk decisions around the specific control implementations they are mandating for implementation to mitigate the risk to USG information in commercial systems. This leads to the very specific requirements with little leeway for organizational risk management. This paper specifically deals with the potential for alternative assessment approaches to the evaluation of control implementation that would provide for maximum risk reduction while limiting the cost of control implementation.

In rolling out its current approach requiring 100% implementation of all controls the DoD faces a number of potential challenges. The difficulty in perfect implementation has not yet fully materialized, but it will. Broadly, the US Defense Industrial base, including many overseas companies, are not prepared for the scope and complexity of these requirements as outlined in the current Cybersecurity Maturity Model Certification (CMMC) assessment methodology. Additionally, the hours required to fully assess each control will severely strain available assessment resources making the scope of

assessments desired unlikely to be realized. This research supports the assertion that a more focused approach can realize the majority of risk reduction for DoD sensitive information, while limiting the burden for implementors and assessors alike. Further research is required to pilot this approach and demonstrate the cost benefit to government regulators.

References

Almeida, Luís, and Ana Respício. "Decision support for selecting information security controls." *Journal of Decision Systems* 27.sup1 (2018): 173-180.

Brotby, W. Krag, and Gary Hinson. *Pragmatic security metrics: applying metametrics to information security*. CRC Press, 2016.

Chidukwani, Alladean, Sebastian Zander, and Polychronis Koutsakis. "A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations." *IEEE Access* 10 (2022): 85701-85719.

Gafni, R. and Levy, Y., 2023. Experts' feedback on the cybersecurity footprint elements: in pursuit of a quantifiable measure of SMBs' cybersecurity posture. *Information & Computer Security*, *31*(5), pp.601-623.

Gandal, N., Moore, T., Riordan, M., and N. Barnir. 2023 "Empirically Evaluating the Effect of Security Precautions on Cyber Incidents", Computers & Security, 133:103380, October 2023.

Gonzales, D., Harting, S., Adgie, M., Brackup, J., Polley, L., and K. Stanley. 2020 "Unclassified and Secure: A Defense Industrial Base Cyber Protection Program for Unclassified Defense Networks", RAND Corporation. Available at https://apps.dtic.mil/sti/tr/pdf/AD1097634.pdf

Gordon, Lawrence A., and Martin P. Loeb. *Managing cybersecurity resources: a cost-benefit analysis*. Vol. 1. New York: McGraw-Hill, 2006.

Strohmier, H., Stoker, G., Vanajakumari, M., Clark, U., Cummings, J., and M. Modaresnezhad. 2022 “Cybersecurity maturity model certification initial impact on the defense industrial base”, *Journal of Information Systems Applied Research*, 15:2, pps. 17-29.

Imsand, Eric, et al. "A survey of cyber security practices in small businesses." *National Cyber Summit (NCS) Research Track*. Springer International Publishing, 2020.

Johnson, Leighton. *Security controls evaluation, testing, and assessment handbook*. Academic Press, 2019.

Karlsson, K., Åström, J., and M. Karlsson. 2015 “Information security culture – state-of-the-art review between 2000 and 2013, Information and Computer Security, July 2015.

Kiesling, Elmar, et al. "Selecting security control portfolios: a multi-objective simulation-optimization approach." *EURO Journal on Decision Processes* 4.1-2 (2016): 85-117.

Levy, Y. and Gafni, R., 2022. Towards the quantification of cybersecurity footprint for SMBs using the CMMC 2.0. *Online Journal of Applied Knowledge Management (OJAKM)*, *10*(1), pp.43-61.

Li, W.W., Leung, A.C.M., and Yue. W.T. Forthcoming. “Where is IT in Information Security? The Interrelationship Among IT Investment, Security Awareness, and Data Breaches,” MIS Quarterly. https://misq.umn.edu/where-is-it-in-information-security-the-interrelationship-among-it-investment-security-awareness-and-data-breaches.html

Merrell Research. 2022 “Defenseless: A statistical Report on the state of cybersecurity maturity across the Defense Industrial Base”, available at https://info.cybersheath.com/Download-Defenseless-The-State-of-the-DIB-merrill-Research.

Moore, T., Dynes, S., and Chang, F. 2016. “Identifying how firms manage cybersecurity investment.” 15th Workshop on the Economics of Information Security (WEIS), available at https://tylermoore.utulsa.edu/weis16cisopres.pdf.

Office of Inspector General (OIG), US Department of Defense. 2019. “Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems”. Available at https://media.defense.gov/2019/Jul/25/2002162331/-1/- 1/1/DODIG-2019-105.PDF.

Office of Inspector General, US Department of Defense. 2022. “Audit of the Protection of Military Research Information and Technologies Developed by Department of Defense Academic and Research Contractors”. Available at https://media.defense.gov/2022/Feb/24/2002944191/-1/-1/1/DODIG-2022-061.PDF

Office of the Secretary of Defense (OSD), US Department of Defense, 2023. " National Defense Industrial Strategy". Available at https://www.businessdefense.gov/docs/ndis/2023-NDIS.pdf

United States Government Accountability Office. 2022. “Defense Cybersecurity: Protecting Controlled Unclassified Information Systems”. Available at https://www.gao.gov/assets/gao-22-105259.pdf

Woods, Daniel W., and Rainer Böhme. "SoK: Quantifying cyber risk." *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021.

Schinagl, S., and A. Shahim, 2020. “What do we know about information security governance? From the basement to the boardroom”: towards digital security governance, Information and Computer Security, January 2020.

Sundararajan, V., Ghodousi, A., and Dietz, J. E. "The Most Common Control Deficiencies in CMMC non-compliant DoD contractors," IEEE International Symposium on Technologies for Homeland Security (HST), Boston, MA, USA, 2022, pp. 1-7, doi: 10.1109/HST56032.2022.10025445.

Yevseyeva, Iryna, et al. "Selecting optimal subset of security controls." *Procedia Computer Science* 64 (2015): 1035-1042.

Tables I-VII

Table I. Information on the Background of Cybersecurity Experts

Respondent	Age	Years of IT Experience	Years of Cyber Experience	Years of Assessment Experience	Years of 800-171 Experience	Years of 800-53 Experience	Years of CMMC Experience
1	55	15	35	15	5	0	3
2	55	26	7.5	16	7.5	0	3
3	73	15	15	15	5	23	3
4	40	18	18	10	10	13	3
5	26	4	3	1	3	0	3
6	42	18	18	8	5	10	3

Table II. Summary Statistics (Benefits, Costs, Values) by 14 Categories of Precautions

	Average Benefit	Average Cost	Average Value All controls	Average Value Controls with Value>0	# of total controls in Category	# Controls with non-positive values in category
Audit and Accountability	3.42	1.75	1.67	1.67	3	0
System and Information Integrity	3.98	2.56	1.33	1.67	7	1
Media Protection	3.53	2.28	1.28	1.28	9	0
Identification and Authentication	3.00	1.61	1.27	1.27	11	0
Personnel Security	3.13	2.00	1.25	1.25	2	0
System and Comm. Protections	3.02	2.68	0.37	1.08	16	7
Access Control	3.07	2.26	0.82	1.07	22	5
Awareness and Training	2.64	2.44	0.33	0.90	9	4
Risk Assessment	4.00	3.00	0.83	0.83	3	0
Maintenance	3.04	2.42	0.63	0.80	6	1
Physical Protection	2.96	2.29	0.67	0.80	6	1
Security Assessment	3.31	2.69	0.44	0.67	4	1
Incident Response	3.08	2.50	0.58	0.58	3	0

Configuration Management	3.47	3.39	0.25	0.50	9	3

Table III: Benefit, Cost and Value for the three constrained optimization exercises

	# of controls	Total Benefit	Total Cost	Total Value	Average Benefit	Average Cost	Average Value
All controls	110	351	265	86	3.19	2.41	0.78
only positive values	87	291	197	93	3.34	2.26	1.07
positive value & benefit >=2.5	76	268	181	85	3.52	2.38	1.12
Top 50 controls	50	178	106	72	3.55	2.11	1.44
best 50 controls + each category with at least 1 control	50	177	105	72	3.54	2.10	1.44
Top 50 controls + each category with at least 25% controls	50	174	103	72	3.48	2.05	1.43
Controls with benefit "5"	44	158	122	36	3.58	2.77	0.83

Table IV. List of Top-50 Controls by Category.

	Total Controls	% of Total Controls	in top-50
Access Control	22	20.0	12
Audit and Accountability	3	2.7	3
Awareness and Training	9	8.2	2
Configuration Management	9	8.2	1
Identification and Authentication	11	10.0	9
Incident Response	3	2.7	1
Maintenance	6	5.5	2
Media Protection	9	8.2	7
Personnel Security	2	1.8	2
Physical Protection	6	5.5	1
Risk Assessment	3	2.7	1
Security Assessment	4	3.6	0
System and Communications Protections	16	14.6	4
System and Information Integrity	7	6.4	5

Table V: Robustness Of Main constrained optimization exercise

	# of precautions	Total Benefit	Total Cost	Total Value	Average Value	Number of Same precautions
Top 50 precautions - exercise #3	50	177.5	105.5	72	1.44	50
Option 1	50	181.2	106.4	74.8	1.50	44
Option 2	50	174.8	108.4	66.4	1.33	41
Option 3	50	173.8	97.6	76.2	1.52	42
Option 4	50	173.5	102.0	69.3	1.39	42
Option 5	50	174.6	105.4	69.2	1.38	41
Option 6	50	178.0	103.2	74.8	1.50	42
All Six Experts	50	179.8	109.0	70.8	1.42	43

Table VI. Top-50 controls

		Benefit	Cost	Value
SI.L1-3.14.2	Provide protection from malicious code at designated locations within organizational systems.	4.75	2.25	2.5
MP.L2-3.8.7	Control the use of removable media on system components.	4.5	2	2.25
SI.L1-3.14.4	Update malicious code protection mechanisms when new releases are available.	3.375	1.5	2.125
SC.L1-3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	4.25	2.25	2
AT.L2-3.2.1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security benefits associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	3.5	1.75	2
AC.L2-3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	4.25	1.75	2
SI.L2-3.14.3	Monitor system security alerts and advisories and take action in response.	4.25	1.75	2
IA.L2-3.5.10	Store and transmit only cryptographically- protected passwords.	3.75	2	1.75
AC.L2-3.1.8	Limit unsuccessful logon attempts.	3.25	1.5	1.75
IA.L1-3.5.2	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	3.75	1.75	1.75

SC.L2-3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	4.25	2.75	1.75
IA.L2-3.5.3	Use multifactor authentication (MFA) for local and network access to privileged accounts and for network access to non- privileged accounts.	4.75	3	1.75
AC.L2-3.1.21	Limit use of portable storage devices on external systems.	3.75	1.75	1.75
SI.L1-3.14.5	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	3.875	2	1.625
PE.L1-3.10.3	Escort visitors and monitor visitor activity.	3	1.5	1.5
SC.L2-3.13.16	Protect the confidentiality of CUI at rest.	4	2	1.5
AT.L2-3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	3.25	1.5	1.5
AC.L2-3.1.17	Protect wireless access using authentication and encryption.	3.5	2	1.5
SC.L2-3.13.15	Protect the authenticity of communications sessions.	3.75	2.5	1.5
IA.L2-3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	2.75	1	1.5
AC.L2-3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	2.5	1	1.5
AT.L2-3.2.2	Ensure that personnel are trained to carry out their assigned information security- related duties and responsibilities.	3.5	2	1.5
AU.L2-3.3.4	Alert in the event of an audit logging process failure.	3	1.5	1.5
MP.L2-3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	3.25	2	1.5
MP.L2-3.8.2	Limit access to CUI on system media to authorized users.	4	2.75	1.5
PS.L2-3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.	2.75	1.75	1.25
MP.L2-3.8.9	Protect the confidentiality of backup CUI at storage locations.	3.25	2.25	1.25
IR.L2-3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	4.25	2.75	1.25
IA.L1-3.5.1	Identify system users, processes acting on behalf of users, and devices.	3.5	2.25	1.25
MP.L2-3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	3.75	2.25	1.25

IA.L2-3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	2.5	1.25	1.25
MP.L2-3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	3.25	2	1.25
IA.L2-3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	3.5	2	1.25
PS.L2-3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	3.5	2.25	1.25
IA.L2-3.5.11	Obscure feedback of authentication information.	2.25	1	1.25
MP.L1-3.8.3	Sanitize or destroy system media containing CUI before disposal or release for reuse.	3.5	2.25	1.25
MA.L2-3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	3	2.25	1.25
AC.L2-3.1.16	Authorize wireless access prior to allowing such connections.	3	1.75	1.25
RA.L2-3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	4.5	2.75	1.25
AC.L1-3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	4.5	3.5	1
AC.L1-3.1.20	Verify and control/limit connections to and use of external systems.	3.5	3	1
AC.L2-3.1.3	Control the flow of CUI in accordance with approved authorizations.	4	3.25	1
AC.L2-3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	4	2.75	1
MA.L2-3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	3.5	2.75	1
PE.L1-3.10.1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals	3.25	2.5	1
AC.L2-3.1.11	Terminate (automatically) a user session after a defined condition.	2.25	1.5	1
AU.L2-3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	3.25	2.25	1
AC.L1-3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	3	2.25	1
IA.L2-3.5.8	Prohibit password reuse for a specified number of generations.	2.25	1.25	1
SI.L2-3.14.7	Identify unauthorized use of organizational systems	3.75	2.75	1

Table VII. 34 precautions with non-positive values or low benefit

		Benefit	Cost	Value
IA.L2-3.5.11	Obscure feedback of authentication information.	2.25	1	1.25
AC.L2-3.1.11	Terminate (automatically) a user session after a defined condition.	2.25	1.5	1
IA.L2-3.5.8	Prohibit password reuse for a specified number of generations.	2.25	1.25	1
AU.L2-3.3.9	Limit management of audit logging functionality to a subset of privileged users.	1.75	1.25	0.75
AU.L2-3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	2	1.5	0.75
IA.L2-3.5.6	Disable identifiers after a defined period of inactivity.	2.25	1.25	0.75
AC.L1-3.1.22	Control information posted or processed on publicly accessible systems.	2	1.25	0.5
AC.L2-3.1.14	Route remote access via managed access control points.	2.25	2	0.5
AU.L2-3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	2	1.5	0.5
IA.L2-3.5.5	Prevent reuse of identifiers for a defined period.	1.75	1	0.5
IR.L2-3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	2.25	2.25	0.25
AC.L2-3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	1	1.25	0
AC.L2-3.1.4	Separate the duties of individuals to reduce the benefit of malevolent activity without collusion.	2.5	2.5	0
AC.L2-3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	3.25	3.25	0
AC.L2-3.1.12	Monitor and control remote access sessions.	3	3	0
AU.L2-3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	3.75	4	0
CM.L2-	Define, document, approve, and enforce physical and logical access	2.75	3	0

3.4.5	restrictions associated with changes to organizational systems.			
CM.L2-3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	3.25	3.5	0
PE.L1-3.10.4	Maintain audit logs of physical access.	2.25	2	0
SC.L2-3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	1.75	1.75	0
SC.L2-3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	2.25	2.5	0
SI.L1-3.14.1	Identify, report, and correct system flaws in a timely manner.	3.625	3.375	0
SC.L2-3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	2.5	2.5	-0.125
AC.L2-3.1.15	Authorize remote execution of privileged commands and remote access to security- relevant information.	1.5	2.25	-0.25
AU.L2-3.3.3	Review and update logged events.	2.5	2.75	-0.25
MA.L2-3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	2.75	2.75	-0.25
CA.L2-3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	3	3	-0.25
SC.L2-3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	3	3.25	-0.25
SC.L2-3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	2.5	2.75	-0.25
AU.L2-3.3.1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	3.25	4	-0.5
AU.L2-3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting.	2.25	3.25	-0.75
CM.L2-3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	3.5	4.5	-0.75
SC.L2-3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	1.75	2.5	-0.75
SC.L2-3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	2.25	4.75	-2.5