The Regulatory Compliance Risks Affecting the Defense Industrial Base

The Risks of CUI Management, SPRS Scoring, Supply Chain Accountability, Cloud Hosting, Incident Reporting, and Export Controls

Introduction

The Defense Industrial Base (DIB) inherently operates under strict regulations to safeguard sensitive information, including Federal Contract Information (FCI), Controlled Unclassified Information (CUI), and Export Control Information (ECI) with the need to ensure cybersecurity standards.

Compliance with the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) are critical for maintaining regulatory, legal, and contractual obligations and ultimately assisting the DoD in meeting its security objectives.

This article explores the risks associated with various aspects of CUI management, including the dangers of over-classifying information as CUI, inaccurately reporting Supplier Performance Risk System (SPRS) scores, responsibilities when sharing CUI within the supply chain, hosting CUI in public cloud environments without FedRAMP Authorization to Operate (ATO), and the risks of not reporting cyber incidents promptly. Additionally, we address the risks associated with treating all CUI as export-controlled and clarify the misconception that CUI should only be accessible by U.S. citizens.

These regulatory risks are compounded by the implications of the Christian Doctrine, the False Claims Act (FCA), and the Defense Contractor Whistleblower Protection Act (DCWPA), which are also discussed in the context of regulatory compliance.

1 Risks of Treating or Marking Everything as CUI

Treating or marking all information as CUI can have significant drawbacks:

OPERATIONAL INEFFICIENCY

Complexity and Delays: Overclassifying information as CUI can lead to unnecessary complexity in handling, storing, and transmitting data. This can slow down processes, create bottlenecks, and reduce overall efficiency. This becomes especially complex when sharing information with outside entities. The overmarking of CUI can place significant strain on your supply chain. Lastly, there is no easy way to determine if/when to report cyber incidents to external agencies, if we do not have a clear understanding of what datasets are in-scope for a given government agency.

Resource Drain: Resources such as time, money, and personnel may be overextended in managing CUI, diverting focus from more critical tasks. This misallocation can strain an organization's capacity to protect sensitive information effectively. If everything is important, then nothing is.

SECURITY RISKS

Complacency and Insider Threats: When everything is treated as CUI, employees may become desensitized to the importance of protecting genuinely sensitive information. This could lead to complacency, where critical data is handled with less care, increasing the risk of insider threats and unauthorized disclosure or release of protected information.

INCREASED NON-COMPLIANCE RISKS AND FINANCIAL LOSS

During security assessments and audits, overclassifying data can make it difficult to demonstrate that appropriate controls are in place for genuinely sensitive information. This could lead to findings of non-compliance during assessments, such as those conducted under the Cybersecurity Maturity Model Certification (CMMC).

If an organization broadly applies CUI markings without proper justification, it may struggle to consistently maintain the required security controls, leading to potential violations of DFARS requirements. This is especially true when using cloud service providers (CSPs) and external service providers (ESPs).

Overprotecting non-sensitive data incurs unnecessary costs for encryption, storage, and access control mechanisms. These costs can accumulate and detract from investments in areas that require more stringent security.

If a breach occurs because critical data was not adequately protected amidst overclassification, the organization's reputation could suffer, leading to loss of trust from the Department of Defense (DoD) and other stakeholders.

2 Risks of Treating All CUI as Export-Controlled Information

Treating all CUI as if it is subject to export control laws, such as the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR), poses significant risks:

OPERATIONAL INEFFICIENCY

Unnecessary Restrictions: Over-classifying CUI as export-controlled information introduces unnecessary restrictions on who can access the data. This can hinder collaboration, delay project timelines, and increase administrative burdens as organizations attempt to manage compliance with export control laws unnecessarily.

COMPLIANCE RISKS

Misapplication of Regulations: Not all CUI is export-controlled, and applying these regulations broadly can lead to confusion and mismanagement of information. Misclassifying CUI as export-controlled could also result in non-compliance with actual export control regulations, leading to potential legal and financial penalties.

Impact on Workforce: The misconception that CUI should only be accessible by U.S. citizens can lead to the exclusion of lawful U.S. persons (which includes lawful permanent residents and other protected individuals under U.S. law) from accessing information they are legally entitled to handle. This not only limits the available talent pool but also violates anti-discrimination laws.

SECURITY RISKS

False Sense of Security: Over-classifying CUI as export-controlled may create a false sense of security, where organizations believe they have implemented more stringent controls than necessary. This could lead to lax enforcement of actual security requirements for genuinely sensitive data.

3 Risks of Inaccurate SPRS Scoring to Achieve 110/110

Accurately reporting your organization's cybersecurity posture in the SPRS is crucial for maintaining trust with the DoD. An inaccurate SPRS score, particularly one that falsely portrays a perfect 110/110, poses several risks:

REGULATORY NON-COMPLIANCE

False Representation: Submitting an inaccurate SPRS score constitutes a false representation of the organization's cybersecurity capabilities. This can lead to non-compliance with DFARS 252.204-7019 and 252.204-7020, requiring accurate cybersecurity readiness reporting.

Legal Consequences: If the inaccuracy is discovered, your organization could face legal action from the DoD, including fines, penalties, or even suspension from current contracts.

CONTRACTUAL RISKS

Breach of Contract: Misrepresenting your cybersecurity maturity through an inaccurate SPRS score may be viewed as a breach of contract, potentially leading to contract termination and financial liabilities.

Failure to Meet Obligations: If your cybersecurity posture is not as robust as reported, it could lead to failures in meeting contractual obligations, especially if the DoD conducts an assessment or audit and finds discrepancies.

INCREASED CYBERSECURITY VULNERABILITIES

Lack of Preparedness: A falsely inflated SPRS score might lead to complacency within the organization, where critical security gaps are overlooked. This increases the risk of cyber incidents that could compromise CUI and other sensitive information.

REPUTATIONAL AND FINANCIAL RISKS

Damage to Reputation: Once the inaccuracy of the SPRS score is exposed, it could severely damage your organization's reputation with the DoD and other partners, leading to a loss of future contract opportunities.

Financial Penalties: Regulatory bodies might impose fines for non-compliance, especially if the inaccurate score is seen as an intentional misrepresentation. These fines, coupled with the cost of remediating the issues, can be financially burdensome.

4 Responsibilities Beyond Flowing Down DFARS 7012

When sharing CUI with supply chain partners, your responsibility extends beyond simply including DFARS 252.204-7012 in contracts. Here's why:

SECURITY RISKS OF SHARING CUI WITHOUT VALIDATION

Exposure to Breaches: If your supply chain partners cannot properly protect CUI, there's a heightened risk of unauthorized access or data breaches, which could have severe national security implications.

Supply Chain Vulnerabilities: Inadequately secured partners can become weak links, making the entire supply chain vulnerable to cyber-attacks. This not only compromises your organization's security but also the integrity of the broader defense supply chain.

REGULATORY AND COMPLIANCE RISKS

Continuous Responsibility: Flowing down DFARS 7012 is not sufficient; you are also responsible for ensuring that your suppliers can comply with the requirements. This means conducting due diligence, ongoing assessments, and requiring suppliers to demonstrate their compliance capabilities.

Legal Liabilities: If a supplier fails to protect CUI and a breach occurs, your organization could be held legally liable. This includes potential penalties, contract termination, and damage to your standing with the DoD.

FINANCIAL AND REPUTATIONAL RISKS

Cost of Breaches: The financial impact of breaches in the supply chain can be substantial, including costs related to remediation, legal fees, and fines. Moreover, your organization might lose revenue if contracts are terminated due to non-compliance.

Reputational Damage: Non-compliance or a breach in the supply chain can significantly damage your organization's reputation, leading to loss of trust and future business opportunities.

5 Risks of Hosting CUI in a Public Cloud Environment Without FedRAMP ATO

Hosting CUI within a public cloud environment or with a cloud service provider that lacks a Federal Risk and Authorization Management Program (FedRAMP) Authorization to Operate (ATO) introduces critical risks:

SECURITY RISKS

Unauthorized Access: Public cloud environments that do not meet FedRAMP standards may not have the necessary controls to prevent unauthorized access to CUI. This increases the risk of data breaches, where sensitive information could be exposed to unauthorized users, including foreign adversaries.

Inadequate Protection: FedRAMP ATO ensures that a cloud service provider has implemented a robust set of security controls aligned with NIST standards. Without this authorization, there is no guarantee that the cloud provider can adequately protect CUI, leaving it vulnerable to cyber threats.

COMPLIANCE RISKS

Violation of DFARS 7012: DFARS 252.204-7012 mandates that CUI must be safeguarded according to specific security requirements, including those outlined in NIST SP 800-171. Utilizing a cloud provider without FedRAMP ATO may result in non-compliance with these requirements, leading to potential legal and contractual penalties.

Risk of Contract Termination: The DoD requires that CUI be stored in environments that meet stringent security requirements. Failing to use a FedRAMP-authorized provider could be seen as a breach of contract, resulting in the termination of current contracts and the loss of future business opportunities.

FINANCIAL AND REPUTATIONAL RISKS

Remediation Costs: If a breach occurs due to the inadequate security of a non-FedRAMP-authorized cloud service provider, your organization could face significant remediation costs, including legal fees, breach notifications, and compensation for affected parties.

Reputational Damage: Exposure to CUI due to inadequate cloud security can severely damage your organization's reputation with the DoD and other defense contractors, leading to a loss of trust and potential exclusion from future contracts.

6 Risks of Not Reporting Cyber Incidents to DIBNet or Prime Contractors

Timely and accurate reporting of cyber incidents is critical to compliance with DFARS 252.204-7012. Failure to report incidents to DIBNet within the required 72-hour window, or not reporting to your prime contractor if you are a subcontractor, carries significant risks:

REGULATORY NON-COMPLIANCE

Violation of DFARS 7012: DFARS 252.204-7012 requires that contractors report cyber incidents that affect CUI to the Defense Industrial Base Cybersecurity Assessment Center (DIBNet) within 72 hours. Failure to report within this timeframe directly violates DFARS, potentially leading to legal and contractual penalties.

Failure to Notify Prime Contractors: If you are a subcontractor, failing to inform your prime contractor of a cyber incident not only violates your contractual obligations but can also disrupt the prime contractor's ability to comply with their own reporting requirements. This can result in cascading non-compliance issues throughout the supply chain.

LEGAL AND CONTRACTUAL RISKS

Potential Legal Action: Non-compliance with incident reporting requirements can lead to legal action from the DoD, including fines, penalties, and contract termination. The DoD takes cybersecurity seriously, and failure to report incidents could be seen as a breach of contract, leading to severe consequences.

Increased Scrutiny: Failure to report incidents as required can trigger increased scrutiny from the DoD, including more frequent audits and assessments. This can further strain your organization's resources and lead to additional compliance challenges.

SECURITY RISKS

Delayed Response and Mitigation: Not reporting cyber incidents promptly can delay the DoD's ability to respond to and mitigate the impact of the incident. This can result in greater damage, including the potential for the incident to affect other parts of the defense supply chain.

Compromise of Sensitive Information: If a cyber incident involving CUI is not reported and properly addressed, it can compromise sensitive information, which adversaries could exploit, leading to national security risks.

REPUTATIONAL AND FINANCIAL RISKS

Damage to Reputation: Failure to report cyber incidents as required can damage your organization's reputation with the DoD and other partners. This loss of trust can lead to difficulties securing and maintaining future contracts.

Financial Penalties: Non-compliance with incident reporting requirements can result in significant financial penalties, including fines and the cost of remediating the incident. Additionally, your organization could face increased insurance premiums and other financial burdens due to the breach.

7 The Christian Doctrine, False Claims Act, and Whistleblowers

By adhering to these guidelines and leveraging the referenced materials, organizations can better manage the risks associated with failing to comply with CUI management, reporting, and regulatory compliance within the DIB:

CHRISTIAN DOCTRINE

Implied Contractual Obligations: The Christian Doctrine implies that certain mandatory clauses, such as DFARS 252.204-7012, are included in government contracts by law, even if they are not explicitly written. This means your organization is automatically bound by these requirements, making non-compliance a breach of contract.

Consequences of Non-Compliance: Failure to comply with the implied requirements can result in severe penalties, including contract termination and legal action. The Christian Doctrine ensures that critical regulatory requirements are enforced, even if they are not explicitly stated in the contract.

FALSE CLAIMS ACT (FCA)

Liability for False Representations: The FCA imposes liability on organizations that knowingly submit false claims or certifications to the government, such as inaccurate SPRS scores or failure to report cyber incidents. Penalties under the FCA can include treble damages and statutory fines.

Whistleblower Protections: The FCA includes provisions that allow whistleblowers to file qui tam lawsuits on behalf of the government if they believe an organization has committed fraud. If an employee or third party becomes aware of an inaccurate SPRS score, failure to report cyber incidents, or other non-compliance issues, they could initiate legal action, leading to significant legal and financial repercussions.

REGULATORY COMPLIANCE AND THE DIB

Ensuring Compliance Across the Supply Chain: Given the implications of the Christian Doctrine and FCA, it's critical for organizations in the DIB to ensure full compliance with all regulatory requirements, not just within their own operations but across their entire supply chain.

Proactive Risk Management: Implementing robust compliance programs, conducting regular audits, and ensuring accurate reporting are essential to mitigating risks associated with regulatory non-compliance. This proactive approach helps to protect your organization from legal, financial, and reputational damage.

Key Takeaways

Many organizations within the DIB have substantial tasks related to managing CUI, accurately reporting SPRS scores, ensuring supply chain security, choosing appropriate cloud environments, and timely reporting cyber incidents.

Organizations within the DIB must comply with DFARS requirements and take proactive steps to validate the cybersecurity readiness of their supply chain partners and service providers. Additionally, understanding the nuances of export control regulations and avoiding the misconception that all CUI must be treated as export-controlled or restricted to U.S. citizens is crucial for maintaining compliance and operational efficiency.

Failure to address these responsibilities can result in significant risks, including security breaches that negatively affect national security objectives, legal liabilities under the Christian Doctrine and False Claims Act, and the potential for whistleblower actions.

By taking a proactive approach to compliance and risk management, organizations can protect their interests, maintain trust with the DoD, and contribute to the security of the defense supply chain.

References

DFARS 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting - https://www.acquisition.gov/dfars/252.204-7012

NIST SP 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations - https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

DoD Cybersecurity Maturity Model Certification (CMMC) - https://www.acq.osd.mil/cmmc/

False Claims Act (FCA) - https://www.justice.gov/civil/false-claims-act

FedRAMP Authorization to Operate (ATO) - https://www.fedramp.gov

Christian Doctrine - https://www.law.cornell.edu/wex/christian_doctrine

International Traffic in Arms Regulations (ITAR) - https://www.pmddtc.state.gov/ddtc_public?id=ddtc_public_portal_itar_landing

Export Administration Regulations (EAR) - https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear

13577 Feather Sound Drive
Suite 420
Clearwater, FL 33762

SP6.io
service@sp6.io
727-353-2360

SP6 Provides Elite Level Compliance Advisory Services Delivered by Certified CMMC Assessors (CCAs) and Certified CMMC Professionals (CCPs).

At SP6, our mission is simple: safeguard your data, slash cyber risk, and secure compliance. Join the ranks of the Fortune 20 companies, state governments, Ivy League Universities and others that are transforming their security posture and simplifying compliance with SP6.

Customer Centric to the Core

Our goal isn't to simply run through a checklist — instead, we take the time to intricately understand each organization's unique situation and objectives so that we can provide customized, ROI-enhancing solutions.