THE AUGUSTA GROUP

The Augusta plan: Thought leadership, implementing cybersecurity and risk management for Federal Agencies and their contractors

Reasserting accountability and responsibility for managing Cyber-SCRM. Leveraging existing regulatory practices including OMB A-130, FISMA, the RMF and CyberSecurity Framework (CSF) profiles.

November 2021 – Version 2.0

Andy Watkin-Child, Ted Dziekanowski

The Augusta Plan

In August of 1941, President Franklin Delano Roosevelt met Prime Minister Winston Churchill for the first time aboard the cruiser U.S.S. Augusta to formulate a strategy for conducting World War Two. Whilst the authors of this paper do not claim the greatness of either leader, our intention is somewhat similar. As was recognized 80 years ago, the securing of the sovereignty of nations against hostile threat actors required a collective effort of nation states. Our solution attempts to leverage existing global standards used to protect one information type (financial data material to accurate reporting of results) to another information type such as sensitive Intellectual Property(IP) while providing appropriate oversight to Federal Agencies in a manner that respects the sovereignty of partner nations.

This paper proposes a strategy that has 8 objectives, that we hope can lead to better protection of the Intellectual Property (IP) of US Federal Agencies and the companies that support them. This can be done utilizing existing Federal regulations that includes FISMA, the Risk Management Framework and Cybersecurity Framework (CSF) Profiles and to secure Federal Supply Chains, while also help support contractors and subcontractors to implement appropriate and proportional cybersecurity risk management processes and cybersecurity practices.

We hope that the strategy outlined in this paper leads to tactical solutions that can help secure critical infrastructure and forms the basis for further efforts in securing other areas of the global economy and regulatory regimes, such as the Securities and Exchange Commissions (SEC) oversight over Environmental Societal and Governance (ESG) reporting.

Executive summary

Cyber-Supply Chain Risk Management (C-SCRM) is an objective of the United States Government in response to numerous and significant cyber-attacks. Cyberattacks on the United States public and private sector increased in 2020 and 2021, GAO, FISMA, and Inspector General reports predicted that these attacks would increase[1-6]. Even though the Federal government has been working to resolve cybersecurity since the passing by Congress of the Federal Information Security Management Act (FISMA) in 2002 and modified in 2014[7] (Modernization), these laws have not been effective in reducing the impact from cyber events[8]. Executive Orders in February and May 2021 directed efforts to manage supply chain risks, with the development of appropriate legislation to enforce C-SCRM across U.S. critical national infrastructure planned in 2021. C-SCRM is not a new issue and was the focus of Congress when they enacted FISMA. FISMA requires the adoption of the Risk Management Framework (RMF, NIST SP 800 - 37R2)[9] by all Federal Agencies, their contractors, and the development of C-SCRM policy, the application of risk management practices that align with both FISMA and Office of Management and Budget (OMB) A-130[10] ('*Managing Information as a Strategic Resource'*). OMB circular A-130 establishes general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources and supporting infrastructure and services, requiring Federal agencies to adhere to the Federal Information Security Modernisation Act. As an example, the DoD is working towards meeting this requirement through the adoption of DoDI 8510.01 (*Risk Management Framework (RMF) for DoD Information Technology (IT))* and DoDI 5000.90 (*Cybersecurity for Acquisition Decision Authorities and Program Managers*).

FISMA and OMB guidance has required the DoD to implement Supply Chain Risk Management (SCRM). The approach that the DoD inadvertently developed to implement the cybersecurity component of SCRM was with DFARS 252.204 - 7012, 7019 and 7020. This illustrates a problem for Federal Agencies that chose to mandate the implementation of 'descriptive' cyber security programs. FISMA requires the assessment, quantification, and mitigation of cybersecurity risks by Federal Agencies. While DFARS 252.204 – 7012 compliance requires the adoption of 'all' 110 NIST SP 800-171 cybersecurity practices, by domestic and international defence contractors and subcontractors, irrespective of the cybersecurity risk to Controlled Unclassified Information (CUI). While the intentions of the two unique approaches are sound, put together they send conflicting messages to Federal contractors across the Defence Industry Base (DIB). We believe these conflicts can be resolved by implementing FISMA as required but also using CSF Profiles to provide the controls taxonomy to not only mitigate cyber-risk but to sharply focus on the mission and business objectives of the contracting agency.

Cyber oversight and assurance are critical for Federal Government Agencies to validate contractor compliance with the intent of FISMA and DFARS to provide adequate cybersecurity. However, there is a problem of not having enough resources to provide the necessary assurance of cybersecurity compliance either nationally or internationally. We believe that this is an issue that can be addressed through the utilization of existing oversight bodies such as the American Institute of Certified Public Accountants (AICPA). These oversight bodies oversee similar frameworks that deal with various information types including financial applications (Sarbanes Oxley), PII (GDPR/ CCPA) and PHI (HIPPA). Another example is the supply chain SOC audit which can provide assurance that supports SSAE18. These audits and assessments are conducted by Certified Public Accountants (CPAs) skilled in both auditing processes and cyber/ IT security. Federal Agencies could request that all Federal contractors submit an appropriate audit certificate, as is already accepted in DoDI 5000.90 for High and Moderate risk tolerance systems. This approach could address oversight and assurance issues including resourcing, reciprocity of assessment and partner Nation oversight.

The risk management and the controls implementation process are expensive. Federal Agencies are required to implement FISMA using a risk-based approach for cybersecurity based upon NIST SP 800–37 (R2), which incorporates the NIST SP 800-53 (R5) control taxonomy as a baseline. The approach used by Federal Agencies is not necessarily that adopted by companies providing products and services to Federal agencies. A strict interpretation by Federal government of the imposition of NIST SP 800-53(R5) controls could lead companies exiting the marketplace resulting in reduced competition and increased supply chain risk with even fewer market participants. SCRM can be costly to manage on the part of both Federal Agencies and the companies subject to regulations resulting from it. One approach to managing these costs is focusing on the use of CSF profiles, consisting of practices specifically defined for industry sectors that form a controls taxonymy used to manage the requirements of NIST SP 800-37(R2) and FISMA compliance. This approach further enables the application of controls based upon the protection of a specific information type (PII, PHI, CUI) in agreement with Federal Agencies and their contractors minimizing the number of controls required to those required under FIPS 199 categorization process.

Contractors may also reduce their costs of managing cyber-risk by implementing CSF profiles and adopting a cloud first strategy. Cloud providers including AWS[11] and Microsoft already support[12] this approach. As an example, AWS services have been accredited under FedRAMP Moderate and ISO 9001/27001/27017/27018 aligned to the CSF. That FedRamp accreditation negates the need, under the proposed CMMC program, for an additional certification whose delay could prevent control inheritance by those companies needing to satisfy DFARS regulations. The Core CSF references security controls from widely adopted, internationally recognized standards such as ISO/IEC 27001, NIST 800-53, Control Objectives for Information and Related Technology (COBIT), Council on Cybersecurity (CCS) Top 20 Critical Security Controls (CSC), and ANSI/ISA-62443 Standards-Security for Industrial Automation and Control Systems. While this list represents some of the most widely reputed standards, the CSF encourages organizations to use any controls catalogue to best meet their organizational needs expanding the possible use of controls not currently recognized. A cloud implementation of the CSF will allow for a flexible cost-effective approach to enable cybersecurity risk management, that can be adopted by all Federal Agencies and their contractors and can additionally align to mission and business objectives, regardless of industry sector or geographic location.

In the following paper we outline 8 objectives and present a cost-effective and efficient solution using existing best practices benefiting Federal Agencies, contractors, and subcontractors. Adopting FISMA, appropriate CSF profiles, and a SOC report, in addition to attesting to the management of cybersecurity risk as required by FISMA, control identification using CSF profiles and control design and effectiveness testing for oversight and assurance.

Objectives: This white paper provides options to address the challenges faced by Federal Agencies, their contractors, and subcontractors. Enabling them to implement Cyber-Supply Chain Risk Management (C-SCRM).

The objectives of this paper are:

Objective 1: To facilitate the implementation of existing cybersecurity and risk management regulations as defined by OMB Circular A-130, FISMA (2014), the RMF and DFARS 252.204-7012, for the management of C-SCRM, cyber-risk and cybersecurity.

Objective 2: Enable Federal Agencies, contractors and subcontractors align their cyber risk management requirements, mission, and business objectives for the protection of information types specific to a Federal Agency contract.

Objective 3: Support the selection and implementation of appropriate and proportionate controls to manage C-SCRM using the RMF and CSF profiles. To provide clarity of what constitutes adequate cybersecurity protection for Federal agencies, contractors, and subcontracts.

Objective 4: To leverage oversight and assurance mechanisms which already exist for risk assessment, control design and effectiveness testing for the oversight and assurance of Federal Agency, contractor and subcontractor cybersecurity and cyber risks.

Objective 5: To rapidly expand the number of assessors capable of providing C-SCRM oversight and assurance of Federal Agencies and their domestic and international contractors.

Objective 6: Encourage cyber control inheritance, to improve cost efficiency and reduce the complexity of cybersecurity oversight and assurance by Federal Agencies of their domestic and international contractors. As encouraged by NIST SP 800-37R2.

Objective 7: Improve contractor, and subcontractor control design, control effectiveness, and reporting on behalf of Federal Agencies.

Objective 8: Enable international reciprocity of cybersecurity standards, oversight, and assurance.

Existing appropriate regulatory models and control assurance frameworks

The Financial services sector is often discussed as having a more mature approach to cyber security and for good reason. Financial markets are global, transactional processing has a range of complexity and volume, from simple low volume to complexity high volume transactions, and we are all dependent on Financial Services. For hackers Financial Services are an obvious target for cybercrime and Nation State hackers.

Banking regulation is a contributing factor to the sectors security posture. Financial Services institutions are regulated to manage risk and protect the stability of global financial markets under the Basel Accords (banks) and Solvency 2 (insurance firms).

Banking regulation has a long history. The Basel Committee on Banking Supervision introduced the Basel Accords in 1988 with Credit risk (Basel I). Market and Operational risk, supervisory oversight, and market discipline (the 3 pillars) in 2004 with Basel II. Basel III updated Basel II introduced in 2010, there is a 4th iteration with Basel IV due for implementation in 2023. The Basel Accords illustrate the recognition of the dynamic nature of risk management in the Financial Services sector.

A key principle of the Basel Accords and Solvency II is the requirement for setting and managing minimum regulatory capital requirements (capital ratio). Capital which institutions are required to hold as a percentage of their Risk Weighted Assets (RWA). Oversight is provided by the Basel Committee on Banking Supervision, regional central banks, and national regulators including the Federal Reserve (US), FSA (UK), and BaFin

Andy Watkin-Child, Ted Dziekanowski, Jason Spezzano, Brian McCarthy

(Germany), all of whom are authorised to manage capital ratios.

Capital ratios are set based upon the effectiveness of institutions to manage Credit, Market, and Operational Risk. The level of capital that regulators require financial institutions is not insignificant and is based on the RWA and "risk appetite" of the institution. The size of the regulatory capital allocated for a global tier 1 bank can be more than $150 billion. By way of example, regulatory capital held by covered UK banks as of Q4 2020 was £2,025 billion for Credit and Counterparty risk, £379 billion for Market risk and £288 billion for Operational risk which includes cybersecurity risk[13].

Financial regulators assess capital holdings through the Supervisory Review and Evaluation Process (SREP) and supervisory stress testing, valuating an institution's management of risk. Evaluating the RWA assumptions, risk assessment processes and capital allocations. Where appropriate, regulators will change capital ratios and capital allocations.

The Risk and Control Self-Assessment Process (RCSA)[14]. The most widely adopted process used by financial institutions for the evaluation of operational Risk (that includes cyber risk) is the RCSA process.

The RCSA requires,

- The identification and assessment of inherent risk.
- The identification and assessment of the effectiveness of controls in place to mitigate inherent risk.
- The documentation and prioritisation of remediation plans to mitigate control weaknesses.

The RCSA requires three key inputs. The first is a documented taxonomy of risks that are known to impact the organisation. The second is a documented taxonomy of the controls that the organisation operates and should operate, to mitigate the impact of the risks identified by the risk taxonymy. The third a documented enterprise architecture, detailing the organisations processes, technology, and organisational structure (people, process, and systems). These inputs form the basis for the risk assessment process that assesses a risk identified from the risk taxonomy and its impact to the organisation people, process, and systems (inherent risk) and the effectiveness of controls in reducing inherent risk to an acceptable and agreed level (residual risk).

The RCSA process mirrors that of FISMA and the RMF (NIST SP 800 - 37R2). Facilitating the effective and efficient management of operational and cyber-risk.

Incentives to Manage Risk: Operational and cyber-risk management are tied to regulatory capital. Capital that financial services are required to hold to manage unexpected and extreme losses, creating an incentive to manage cybersecurity. Demonstrating to regulators that operational and cyber-risks are effectively managed if they want Tier 1 capital allocations to be reduced. Using the RCSA process as a mechanism to demonstrate the effective management of risk. Freeing capital allocated for risk management on the balance sheet for other uses, increasing profit and optimising shareholder value.

Sarbanes Oxley 2002: SoX is a source of regulatory oversight for publicly traded companies, that can include DIB contractors. SoX compliance requires the leadership of public companies registered in the US to individually attest to the accuracy of financial information and the management of material financial controls.

The act established the Public Company Accounting Oversight Board (PCAOB) that is charged with overseeing, regulating, inspecting, and disciplining accounting firms in their roles as auditors of public companies.

SoX section 404 requires management and their external auditors to produce an "internal control report". Affirming the responsibility of management in establishing and maintaining an adequate internal control structure and procedures for financial reporting.

Assessing the effectiveness of the internal control structure and procedures of financial reporting requires management to:

- Assess the design and operating effectiveness of selected internal controls related to significant accounts in the context of material misstatements.
- Document transaction flows, including IT.
- Evaluate entity level controls, controls designed to prevent fraud and period ending financial reporting processes.
- Conclude on the adequacy of internal control over financial reporting.

SoX requires covered organisations to undertake an annual financial audit, assessing material process level and IT general controls which impact financial processing.

SoX has been a contentious act for smaller entities. In many ways with similarities to DFARS and the DIB, mandating regulatory oversight and independent assurance of US public companies. SoX provides investors with a level of confidence in an organisations leadership to manage its material financial entity, process, and IT general controls. SoX provides a minimum level of confidence in organizations' ability to manage effective- security processes and controls to manage their cyber risks under IT General Controls testing.

Trust Services Criteria (TSC) and System and Organization Control (SOC) Audits

Federal government relies upon complex domestic and international supply chains. Made up of organisations that must adhere to global financial reporting standards and frameworks including SoX, IFRS and GAAP to assess corporate economic efficiency, and improve capital allocation. Lowering the cost of capital and reducing international reporting costs. Standards which rely on an organisations controls framework to manage the design, manufacture, sale and servicing of products and services.

A source of appropriate international cybersecurity oversight for Federal Agencies and contractors has been created by the American Institute of Certified Public Accountants (AICPA). The AICPA has created a framework, called the Trust Services Criteria (TSC), to be used to evaluate the suitability of the design and operating effectiveness of controls, relevant to the security, availability, or processing integrity of information and systems. TSC is aligned to COSO principles and the NIST Cybersecurity Framework, NIST SP 800–53, ISO 27001, COBIT 5 and GDPR[8].

The TSC provide an evaluation and reporting framework that companies of all types and sizes can use to report on their security, availability, and processing integrity controls, regardless of which specific security regulations they have to comply with. In that way, SOC reports provide information that enables comparability. Whilst a SOC audit is not mandatory for public companies it provides stakeholder assurance of an organisation’s management of key controls.

Federal Government and contractors need to provide as much information as is practical and possible to manage their cybersecurity risks and validate their compliance with FISMA requirements. To do so the information needs to reflect the control design, control effectiveness and on-going and continual nature of control performance. A single-point-in time assessment does not provide adequate assurance of controls effectiveness. Some of the current and available mechanisms to provide this information include.

- SoC 1 - *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting*,
- SoC 2 – *Reporting on an examination of Controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users’ data and the confidentiality and privacy of the information processed by these systems.*
- SoC 3 - *As per a SoC 2 report, but can be freely distributed.*

- SoC for cybersecurity - *Reporting on the effectiveness of an organization's cybersecurity risk management program.*
- SoC for Supply Chain – *Reporting on an entity's system and controls for producing, manufacturing, or distributing goods and the cybersecurity risks in their supply chains.*

SOC reports provide a verifiable auditing report which is performed by a Certified Public Accountant (CPA) designated by the American Institute of Certified Public Accountants (AICPA). Following a process that adheres to Statement on Standards and Attestation Engagements 19 (SSAE18).

SOC reports can be provided globally using reciprocal arrangements that exist between global accounting regulators and accounting firms. Accounting firms who have relationships with DIB Prime contractors and subcontractors through their financial audit processes.

A SOC 2 report is identified in DoDi 5000.90 as an accepted assessment of manufacturers of DoD weapon systems. Where the Program Manager (PM) has determined that there is a high or moderate risk tolerance for a given weapon system.

Recommendations to protect Federal IP and contractors

Existing Federal regulations and standards provide the tools to manage cyber-risk and secure Federal data if implemented appropriately by Federal Agencies and their domestic and international contractors, and subcontractors. The regulations that cause compliance and legal risk to organisations include.

- Federal Information Security Modernization ACT 2014 (FISMA) and the Risk Management Framework (NIST SP 800 - 37R2).
- Office of Management and Budget (OMB) Circular A-130.
- DFARS 252.204-7012, 7019 and 7020.
- False Claims Act.

Enforcement regimes defined by:

- The Department of Justice (DoJ), civil fraud initiative utilizing the 'False Claims Act'.
- The Department of Defence required DFARS compliance ahead of the awarding of a contract or options.
- The Securities and Exchange Commission (SEC) requirements to report material risks including cyber.

OMB A-130 and FISMA are foundational regulatory drivers for cybersecurity compliance by Federal Agencies. Under FISMA §3552 and §3554, the Federal Agency's responsibility is to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of -

(i) Information collected or maintained by or on behalf of the agency.

(ii) Information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

Following the risk management framework (RMF) defined by NIST SP 800 - 37R2.

OMB A-130 establishes general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources and supporting infrastructure and services.

Where DFARS 252.204-7012, 7019 and 7020 have been applied by the DoD to contractors and subcontractors. They are required to implement all 110 NIST SP 800 - 171 cybersecurity practices for the protection of Controlled Unclassified Information CUI. To Flow down these requirements from Prime contractors to contractors and subcontractors (DFARS 252.204-7012). DFARS 252.204-7019 and 7020 requires contracts and subcontractors to inform the DoD of their NIST SP 800-171 compliance score prior to awarding a subcontract and prepare for a possible assessment of their cybersecurity compliance by the DoD.

The following is a discussion of 10 steps that Federal Agencies and the contractors could take under existing regulations to manage cyber risks, provide oversight and assurance of the cybersecurity controls. Ahead of enforcement actions being applied by the Department of Justice, Department of Defence.

1 – Compliance with the requirements of FISMA and the RMF: By Federal Agencies and their contractors. Federal agencies and contractors to Federal Agencies are required to implement NIST SP 800 - 37R2 (RMF) to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of Federal information. This places the responsibility on Federal Agencies and their contractors to manage cybersecurity risk using the NIST SP 800 - 37R2 standard.

NIST SP 800 - 37R2 adopts a similar process to that described under the Risk Control Self-Assessment (RCSA) process. Establishing a strategy for organisation-wide risk management and a risk management framework, steps, and structure to manage cyber-risk for information systems and organizations.

2 – Product specific CSF profiles and contracts: Federal Agency contracts should include an agreement as to the threats to the information types such as CUI or PII held by the Agency and their contractors and subcontractors; agency, contractor and subcontractor mission and business objectives and the environment of operation where data may reside; the threats and vulnerabilities to systems to create a Cybersecurity Framework Profile (CSFP).

Federal Agencies, contractors and subcontractors create a risk-based "Bill of Materials" (BoM) for their products or services. Identifying the cybersecurity risk associated with systems and subsystems within the BoM. This gives flexibility to the Prime to identify components considered high, medium, and low risk. Creating an appropriate cybersecurity risk profile and prioritising the level-of-effort and cost of assurance within its supply chain.

As an example, under the DoD Risk Management Framework (RMF) the DoD is required to risk assess the weapon systems product lifecycle. Under DoDI 5000.90 PMs at their discretion can tailor baseline controls based upon operational requirements. Creating bespoke risk profiles supports the deployment of the RMF into the supply chain and a risk based 'bill of materials' reduces the cybersecurity risk oversight and assurance of the weapon system. E.g. an aircraft's PIT system has a higher cybersecurity risk than its undercarriage.

3 – Accountabilities and responsibilities: Federal Agencies, contractors and subcontractors are accountable and responsible for maintaining cybersecurity of their supply chains, associated with their products and services. Subcontractors perform the same tasks on behalf of their contractors. Creating flow down of cybersecurity oversight and assurance.

Federal Agencies are required to implement a Supply Chain Risk Management Strategy, as defined in NIST SP 800-37R2 for both the Organisation and specific systems being assessed for authorization. This requires flow-down of NIST SP 800-37R2 and agreed CSF profiles through their supply chain.

4 – Oversight and assurance (Contractor): Federal Agencies, contractors and subcontractors assume responsibility for baseline control compliance to CSF profiles and any other controls deemed necessary to reduce risk as defined by NIST SP 800-37R2.

Federal Agencies, contractors and subcontractors are accountable and responsible for assessing compliance. Managing oversight and assurance to the associated CSF profiles, within the terms of the Federal contract.

A Federal Agency could use as an assessment of a contractor and by extension a subcontractor, a SOC report or equivalent, based upon the risk tolerance of the organization of the system in question.

Oversight and assurance of contract compliance is a continual process provided by a SOC report. As opposed to a point in time assessment. A SOC audit could be completed annually and contain all the appropriate information needed to assess cybersecurity compliance.

Federal Agencies, contractors and subcontractors could take a risk-based audit approach to selectively assess compliance with the CSF profiles specified in the contract. Performing on-site assessments based upon the risk tolerance of the agency.

5 – Remediation: Where gaps in compliance have been identified by the agency, contractors, or subcontractors, they are to be remediated following a risk-based approach.

Federal Agencies, contractors and subcontractors are to manage and oversight POAMS within their supply chain, ensuring that they are kept up to date, and milestones achieved. POAMS will be made available to Authorizing Officials (AO) and Program Managers (PM) as required. Contractors and subcontractors will provide an aggregated POAM of all subcontractors for the contract to Federal Agencies.

6 – Oversight and assurance (Federal): It is not practical to assess every single organization. Federal Agencies should sample inspect contractors annually to provide assurance of cybersecurity framework profile contract compliance. Agency Inspector General could selectively assess contractors. The GAO could selectively assess Federal Agencies

7 – Oversight and assurance (complying with FISMA and RMF requirements): The Office of Management and Budget (OMB) and the Office of the Agency's Inspector Generals will assess the compliance Federal Agencies. FISMA assessments are required annually or can be driven sooner by changes to the risk profile of the Agency caused by advanced persistent threats. Reporting of FISMA compliance is made to OMB, CISA and Congress for evaluation.

8 – Congress: Congress can write legislation to remediate gaps identified through OMBs oversight and provide incentives to the supply chain to manage supply chain cyber risks through subsidies. An example of this is evidenced by the proposed FISMA 2021 legislation that among other things proposes change to incident management and reporting requirements.

9 – Performance based incentives/ penalties: As with Basel and Sarbanes Oxley, penalties and incentives are required to facilitate the program. Federal Agencies, contractors and subcontractors should be held accountable for compliance to the appropriate CyberSecurity Framework profile. If a CyberSecurity Framework profile is written into a contract by the Federal Agency, compliance to the contract will be assessed with failure to live up to the terms of the contract possibly falling under the False Claims Act (FCA), that is enforced by the Department of Justice (DoJ).

10 – Adaptive Risk Management (ARM)

The risk management life is continuous, not a one-off or single point in time initiative. The conditions for an on-going authorization of a system (ATO) require the continual assessment and mitigation of risk using an appropriate risk management framework such as NIST SP 800-37R2.

The data collected as part of the risk assessment process is beneficial to agencies that are responsible for the oversight of the FISMA program (CISA). This data provides a level of assurance over the management of the risks associated with the protection of the numerous information types processed by Federal Agencies and provides assurance that federal Agencies understand the risks, threats and vulnerabilities associated with the protection of critical infrastructure. Documenting the controls and their design and effectiveness at mitigating those risks.

Recommendations to address objectives 1 - 8

Objective 1: To facilitate the implementation of existing cybersecurity and risk management regulations as defined by OMB Circular A-130, FISMA (2014), the RMF and

DFARS 252.204-7012, for the management of C-SCRM, cyber-risk and cybersecurity.

- FISMA is a requirement for Federal Agencies, their contractors, and subcontractors.
- Federal Agencies, contractors and subcontractors are required complying with FISMA, implement NIST SP 800-37(R2) and implement a SCRM strategy.
- Contractors and their subcontractors should understand the Departments of Justices utilization of the False Claims Act (FCA) and potentially the enforcement of OFAC should an information type being processed by a contractor or subcontractor be subject to a Ransomware Attack.
- CSF profiles should be used and aligned to business and mission objectives. Providing a flexible and appropriate control's taxonomy. Enabling a cost-effective risk-based approach to the implementation of cybersecurity controls required under FISMA and other regulations specified by Federal Agencies for example DFARS.
- Existing independent oversight and assurance using audit standards, programs and regulated CPAs should be used to assure compliance of FISMA, NIST SP 800 - 37 (R2) and DFARS 252.204 - 7012.

Objective 2: Enable Federal Agencies, contractors and subcontractors align their cyber risk management requirements, mission and business objectives for the protection of information types specific to a Federal Agency contract.

- As per objective 1.

Objective 3: Support the selection and implementation of appropriate and proportionate controls to manage C-SCRM using the RMF and cybersecurity framework (CSF) profiles. To provide clarity of what constitutes adequate cybersecurity protection for Federal agencies, contractors, and subcontracts.

- As per Objective 1.
- Define and agree Federal Agency, industry sector or organization specific CSF profiles that include governance, strategy, risk, and business environment practices for a given information type or types. E.g., NISTIR 8183.

Objective 4: Leverage the oversight and assurance mechanisms which already exist for risk assessment, control design and effectiveness testing for the oversight and assurance of Federal Agency, contractor and subcontractor cybersecurity and cyber risks.

- The global financial audit community completes SOx and Financial audits of regulated organizations. Mandating the submission of a SOC report completed by qualified CPAs will provide contractors and subcontractors with independent assurance of their cybersecurity compliance.
- There are thousands of CPAs in the US qualified to complete assessments. Who can work with cybersecurity professionals, including those who are certified information security professionals (CISA, CISSP, CCSP, CCAK)?
- Reciprocity of oversight can be delivered globally across the DIB using equivalent qualified auditors.
- CPAs and their equivalents are governed by an appropriate regulatory body.
- Cloud providers who are SOC compliant, CSA Star certified and FedRamp certified will be able to make common controls available to contractors and subcontractors for controls inheritance.

Objective 5: To rapidly expand the number of assessors capable of providing C-SCRM oversight and assurance of Federal Agencies and their domestic and international contractors.

- Federal Agencies and major representative of audit firms should agree on the appropriate amount of information, required by a Federal Agency for oversight and assurance of the security of the information types held by a contractors and subcontractors.

Objective 6: Encourage cyber control inheritance, to improve cost efficiency and reduce the complexity of cybersecurity oversight and assurance by Federal Agencies of their domestic and international contractors. As encouraged by NIST SP 800 - 37R2.

- Adoption of CSF profiles enables the alignment of controls between Federal Agencies, contractors, subcontractors, and cloud providers. Facilitating the shared responsibility model and controls inheritance.
- The adoption of an appropriate SCRM strategy and the management of cybersecurity by contractors and subcontractors on behalf of Federal Agencies facilitates the management of the chain of custody of agreed information types that are specified in contracts.
- Federal Agencies, contractors and subcontractors can manage inherited controls using public or private cloud. Understanding the implications of the shared responsibility model and managing customer requirements, will help reduce oversight and assurance requirements across the supply chain, and simplifying contractor and subcontractor audits.

Objective 7: Improve contractor, and subcontractor control design, control effectiveness, and reporting on behalf of Federal Agencies.

- The implantation of FISMA and the RMF requires the implementation of appropriately designed and effective controls to mitigate risk.
- Independent audits performed by CPAs provides objective analysis, findings, and conclusions to assist management and those charged with governance and oversight with, among other things, improving program performance and operations, reducing costs, facilitating and decision making.
- The CPA auditor should report on internal control and compliance with provisions of laws, regulations, contracts, or grant agreements regardless of whether they identify internal control deficiencies or instances of noncompliance.

Objective 8: Enable international reciprocity of cybersecurity standards, oversight, and assurance.

- Federal Agencies, contractors and subcontractors should support the international implementation of FISMA, facilitating a risk-based approach to cybersecurity oversight and assurance.
- Federal Agencies, contractors and subcontractors should support the international adoption of cybersecurity standards based upon CSF profiles that are tailored to information types.
- Establish international oversight and assurance standards for cybersecurity and cyber-risk management using AICPA SoC audits.

Conclusion

Cyber-Supply Chain Risk Management (C-SCRM) is an extremely critical objective of the United States Government in response to numerous and significant cyber-attacks. Cyberattacks on the United States public and private sector increased in 2020 and 2021. GAO, FISMA, and Inspector General reports even predicted that these attacks would increase[1-6]. Even though the Federal government has been working to resolve cybersecurity (Information) since the passing by Congress of the Federal Information Security Management Act (FISMA) in 2002 and modified in 2014[7] (Modernization), these laws have not been effective in reducing the impact from cyber events. Several Executive Orders in 2021 direct efforts to supply chain risks, with the development of appropriate regulations to enforce C-SCRM across the U.S. critical national infrastructure. C-SCRM is not a new issue and had been focused on by Congress when they enacted FISMA. FISMA requires the adoption of the Risk Management Framework (RMF, NIST SP 800 - 37R2)[8] by all Federal Agencies and their contractors.

NIST SP 800 - 37R2 requires organizations to develop a C-SCRM policy and address C-SCRM goals and objectives in their strategic plans, missions, business functions, and organizational roles and responsibilities. The development of C-SCRM policies applies risk management practices that align with both FISMA and Office of Management and Budget (OMB) A-130[9]. Prioritizing C-SCRM and cybersecurity risk management across Federal Agencies, is critical to identifying and mitigating the risk that cyber threats pose to those agencies and the potential impact on their systems.

"FISMA and OMB A-130 require external providers handling federal information or operating systems on behalf of the federal government to meet the same security and privacy requirements as federal agencies. Also, the controls for systems processing, storing, or transmitting federal information are in contracts or other formal agreements. The RMF can be effectively used to manage supply chain risk and OMB A-130 requires organizations to develop and implement SCRM plans."[8]

Cyber risk management

The Office of Management and Budget (OMB) circular A-130 ('Managing Information as a Strategic Resource') establishes general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources and supporting infrastructure and services. Requiring Federal agencies to adhere to the *Federal Information Security Modernisation Act* (FISMA – 2014) and implement an agency-wide risk management process that frames, assesses, responds to and monitors information security and privacy risk on an ongoing basis across their organization, mission or business processes and information systems. Using NISTs Risk management Framework (*NIST SP 800 – 37(R2)*) that provides the Federal framework for the identification, assessment, mitigation, oversight, and assurance of an organisation's cybersecurity risks. The DoD is working towards meeting this requirement through the adoption of DoDI 8510.01(*Risk Management Framework (RMF) for DoD Information Technology (IT))* and DoDI 5000.90 (*Cybersecurity for Acquisition Decision Authorities and Program Managers*). Cybersecurity risks that should be assessed prior to the application of cybersecurity controls (i.e., NIST SP 800–171, NIST SP 800-53, ISO 27001 or a CSF Profile), if efficient and cost-effective risk management is to be achieved.

The adoption of FISMA and the requirement of US Defence contractors to implement DFARS 252.204 - 7012, 7019 and 7020 creates a problem for the DoD or in the case of other Federal Agencies that chose to mandate the implementation of 'Descriptive' cyber security programs. On one hand FISMA requires the assessment, quantification, and mitigation of cybersecurity risks by Federal On the other hand DFARS 252.204 – 7012 compliance requires the adoption of 'all' 110 NIST SP 800-171 cybersecurity practices, by domestic and international defence contractors and subcontractors, irrespective of the cybersecurity risk to Controlled Unclassified Information (CUI). The intentions of the two approaches in case of the DoD to secure CUI are sound. FISMA requires an assessment of risk prior to the selection and implementation of controls while the application of DFARS 252.204-7012 (*Safeguarding covered defence information and cyber incident reporting*) by Federal agencies and their contractors. Mitigating risks using appropriate controls such as those identified by NIST SP 800 - 171 or NIST SP 800 – 53 require the implementation of controls prior to risk assessment. However, FISMA (2014) and OMB A - 130 take precedence over DFARS. The oversight and assurance of both FISMA and DFARS and the efficient and cost-effective implementation of cybersecurity practices by defence contractors through controls inheritance and the shared responsibility model.

Cyber Oversight and Assurance

There are not enough resources to assure cybersecurity compliance nationally or internationally. An issue which can be addressed through existing regulatory bodies, who oversee similar frameworks such as Sarbanes Oxley and System and Organization Control (SOC) 1 and 2. The American Institute of Certified Public Accountants (AICPA) has created Trust Services Criteria (TSC) aligned to COSO, the NIST Cybersecurity Framework (CSF), NIST SP 800–53, ISO 27001 and COBIT 5. SOC reports are designed to provide information to users of outsourced service providers with information about the effectiveness of the service providers' controls over the security, availability, and confidentiality of information processed by those systems. Prepared by independent Certified Public Accountants (CPAs) skilled in both auditing processes and cyber/ IT security, SOC reports reduce compliance burdens by providing one report that addresses the shared needs of multiple users. Today, 5 of the top 14 IT security consultants are CPA firms; there are thousands of qualified CPAs that perform SOC audits. Federal Agencies can request that contractors submit a SOC 2 report, as part of their annual financial audit process? Addressing several oversight and assurance issues including resourcing, reciprocity of assessment and partner Nation oversight and assurance.

Data and Common Control Accountability and Responsibility

Federal agencies rely upon contractors to provide a very broad range of products and services. Products and services that if compromised by a cyber-attack could enable hackers to gain access to Federal systems (SolarWinds and Kaseya) or expose critical sensitive federal data. Data that is used for example to manufacture complex weapon systems in the form of Controlled Unclassified Information (CUI) and must be secured across complex, global supply chains. The Federal Government can oversight and assure its data by adopting a risk-based approach for cybersecurity in line with NIST SP 800 – 37 creating CSF profiles. Identifying the appropriate number of cybersecurity controls required for each contract and request Prime contractors to provide oversight and assurance of these controls across the supply chain. Federal Agencies can allow contractors to implement controls based upon risk and enable contractors to manage controls based upon a cloud shared responsibility model. Simplifying the number of controls requiring oversight and requesting that each contractor and subcontractor provide an annual SOC 2 report, assessing cybersecurity framework profile control design and effectiveness. Placing appropriate data in the cloud and applying controls at the source. This will simplify the chain of custody of Federal Government data, increasing data security, efficiency, effectiveness and reduce the cost of control oversight and assurance.

We address these concerns and present a cost-effective and efficient solution using existing best practices benefiting Federal Agencies, contractors, and subcontractors. By supporting FISMA requirements, creating the appropriate cybersecurity framework profiles based on business and mission requirements, and adoption of a SOC style report we not only address the current problems around C-SCRM but also help organizations lay the foundation for dealing with forthcoming requirements around ESG and other compliance related requirements across multiple information types including PII.

References

1. Government Accountability office (2018): Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities
2. Government Accountability office (2018): Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation
3. Government Accountability office (2021): WEAPON SYSTEMS CYBERSECURITY Guidance Would Help DOD Programs Better Communicate Requirements to Contractors
4. Government Accountability office (2021): Drive to Deliver Capabilities Faster Increases Importance of Program Knowledge and Consistent Data for Oversight
5. Office of the Inspector general US DoD (2019): Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems DODIG-2019-105
6. Government Accountability office (2020): 2020 Defense Acquisition Assessment
7. Federal Information Security Modernization Act (FISMA) – 2014: https://www.congress.gov/bill/113th-congress/senate-bill/2521/text
8. Homeland Security and Governmental Affairs Committee report on FISMA compliance (August 2021): https://www.hsgac.senate.gov/media/minority-media/new-bipartisan-portman-peters-report-shows-federal-agencies-cybersecurity-failures-leaving-americans-personal-information-at-risk
9. Risk Management Framework (NIST SP 800 - 37R2): https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
10. Office of Management and Budget Circular A 130: https://www.cio.gov/policies-and-priorities/circular-a-130/
11. AWS Cybersecurity Framework profile: https://d1.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.pdf
12. Microsoft Cybersecurity Framework profile : https://docs.microsoft.com/en-us/azure/compliance/offerings/offering-nist-csf
13. Basel III UK banks regulatory capital: https://www.bankofengland.co.uk/statistics/banking-sector-regulatory-capital/2020/2020-q4
14. Example RCSA process: https://financialservices.royalcommission.gov.au/public-hearings/Documents/exhibits-2018/23-april/EXHIBIT-2-174-119.pdf