The regulatory cyber-risk elephant in the room, impacting the management of Federal cybersecurity

Federal Government and organizations delivering products and services to Federal Government are regulated to manage cyber-risk.

September 2021

Author: Andy Watkin-Child, Ted Dziekanowski

Contributor: Jason Spezzano, Brian McCarthy

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 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.

The RMF 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. OMB A-130 also requires organizations to develop and implement SCRM plans."[8]

The Department of Defense (DoD) issued DoDI 8510.01[10] (under the authority of the DoD CIO - DoDD 5144.02), requiring the implementation of the RMF in any authorization decisions that allow a system to be placed on its networks. To address the FISMA Congressional mandate applicable to all Federal Agencies. DODD 5000.02T prescribes DoDI 5000.90[11] and DoDI 5000.83 to address the application of the RMF within the Defense procurement life. In addition, DFARS 252.204 - 7012[12], 7019, 7020, and 7021 are to assure adequate security within the Defense Industrial Base (DIB). In alignment with DoDi 8510.01, Air Force instruction AFI 17 – 101[13] (*Risk management framework (RMF) for Air Force - Information Technology)* is an example RMF that meets those requirements.

Under FISMA Federal agencies and contractors to Federal Agencies must also implement the 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. Placing the onus on Federal Agencies and contractors to manage cybersecurity risks. Requiring the oversight and assurance of cyber-risk across the design, manufacturing, and support of products and services supplied to those agencies.

The DoD needs to refocus its efforts on delivering FISMA and NIST SP 800-37R2. Along with evaluating the potential reciprocity offered by other control frameworks, such as Trust Service Criteria (TSC) and the integration of Cybersecurity Framework (CSF) Profiles in Cyber Supply Chain Risk management (C-SCRM). As yet the Current CMMC proposal is not risk based and does not align with FISMA or the DoD RMF program.

We contend that Federal Government has the necessary cybersecurity regulation in place to manage cyber-risk.

The cyber-risk elephant in the room– driving US cyber regulation

Cybersecurity is one of the biggest non-financial risks faced by the United States Government. The World Economic Forum (WEF) in their report on the 'Principles of board governance of cyber-risk'[14], released in March 2021 identifies 'cybersecurity failure' as a top five global short-term risk behind Infectious disease, livelihood crisis, and extreme weather events. In July 2016, NATO formally recognized cyberspace as a legitimate domain of operation[15] reaffirming in April 2021 that cybersecurity is a key part of NATOs core task of collective defense. However, we all have a responsibility for cyberspace and if cyberspace is a legitimate domain of operation, we are all on the battlefield.

The economic impact of a cyber breach can be broad and deep, when targeted at specific parts of Critical National Infrastructure. As demonstrate by the 2020/ 2021 SolarWinds, Colonial Pipeline and JBS Meat cyber-attacks. Attacks can be indiscriminate, often using scripting and automation. A random attack can learn as it deploys, exploiting unremediated risks and spreading uncontrollably. Cyber-risks are as broad and deep as the data an organization creates, processes, stores, or transmits. The impact of a cyber-attack is dependent upon its vulnerabilities and are dependent on:

- The organizations physical and digital perimeter which are often extended into cloud environments.
- The complexity of the products and services an organization manufactures and supplies.
- The number of people a company employs and the number of IT assets they use.
- The organization's dependence on digital products and services.
- The maturity of the cyber threat the organization faces, which can be a nation-state, cybercriminal, hacktivist, or script kiddie.
- The size of the balance sheet.
- The maturity of its cyber-risk and cybersecurity program.
- The reconnaissance a hacker has undertaken on the organization.
- The regulatory environment in which the organization operates.

There is clear evidence of the cyber threat posed by nation-state and their proxies. Nation-state attacks are increasing in their frequency, complexity, and severity. Cyber-attacks have resulted in the loss of Intellectual Property (IP) of organizations, the destruction of digital assets through ransomware, damage to brand and reputation, impacting competitive advantage and National Security. Cyber-attacks potentially impact the security of DoD weapons systems, the critical infrastructure supporting the DIB, and the loss of IP critical to national security. A threat that is recognized by the DoD.

The DIB consists of predominantly small businesses[16] (employing less than 500 people), private sector, national and international organizations. The U.S. Government Accountability Office (GAO) and Office of the DoD Inspector General (DoD IG) have highlighted the challenges faced by the Department of Defense (DoD) in securing its Intellectual Property (IP) and the failure to embed cybersecurity across the DIB, manage weapon system vulnerabilities and protect DoD weapon systems from cyber-attack. The reports are alarming to the Federal Government when the DoD and DIB are subsidizing other nation-states to create their weapon systems. Cybersecurity is an expensive enterprise-wide risk to manage, with the average cost of a cyber-attack increasing significantly over the past 2-years. Ransomware is the prevalent cyber threat vector; the average cost of a cyber-attack has risen to $1.85 Million in 2021 ($700,000 in 2020[17]).

Cyber insurance is the predominant mechanism used by small businesses to mitigate cyber risk. However, the price of cyber insurance has risen over the past year, spiking 32% higher between June 2020 and June 2021. The rise in ransomware attacks has pushed the number of cyber insurance claims up; however, capacity is down and the insurance industry is under pressure to deliver products and manage re-insurance exposure[17].

The US is moving rapidly ahead with cyber regulation. Cybersecurity and Supply Chain Risk Management (SCRM) Executive Orders (EO) were signed in 2021. Regulation established in May 2021 now enables the Securities and Exchange Commission (SEC) to provide oversight of Environmental, Social, and Governance (ESG) material risks. This is in addition to the assessment of the management of financial controls under Sarbanes Oxley (SOx) and other market specific regulations. ESG reporting will include the oversight and assurance of cybersecurity as a material risk.

Foundational risk management pillars for U.S cyber regulation

Cyber and information security laws and regulatory requirements for Federal Government Agencies are underpinned by several pillars. These pillars have been enacted through Congress (FISMA), with oversight (OMB) and required guidance (NIST), which in our opinion should be considered foundational. These pillars consist of.

- The Federal Information Security Modernization Act (*FISMA*) - 2014.
- The Office of Management and Budget (OMB) Circular A-130 *Managing Information as a Strategic Resource.*
- The Risk Management Framework (*RMF – NIST SP 800 – 37R2*).

These pillars are the building blocks for information systems security and risk management across the Federal Government. Cited by other related Federal regulations and standards like the DoD RMF program (DoDI 8510.01), FedRAMP, NIST SP 800-171R2, and NIST 800-53R5.

To understand the importance of FISMA, OMB Circular A-130, the RMF and ultimately the success or failure of cybersecurity management, it is important to understand risk management practices. The risk equation is not complex, but it requires an understanding of an organization's inherent risk profile - an assessment of control design and effectiveness, and the calculation of residual risk. The inherent risk profile is assessed in line with the agreed risk appetite.

The calculation of inherent risk is based upon the assessment of **expected, unexpected and extreme losses** (Figure 1). **Expected losses** are known by an organization and will occur in its daily business, and invariably budgeted into its products and services. **Unexpected losses** are from predictable events which an organization may not have considered and must find the capital or insurance to manage. **Extreme losses** are those an organization 'may' incur and are rare, sometimes known as 'black swan events'. Events that organizations have no means to mitigate and should prepare an incident response plan.

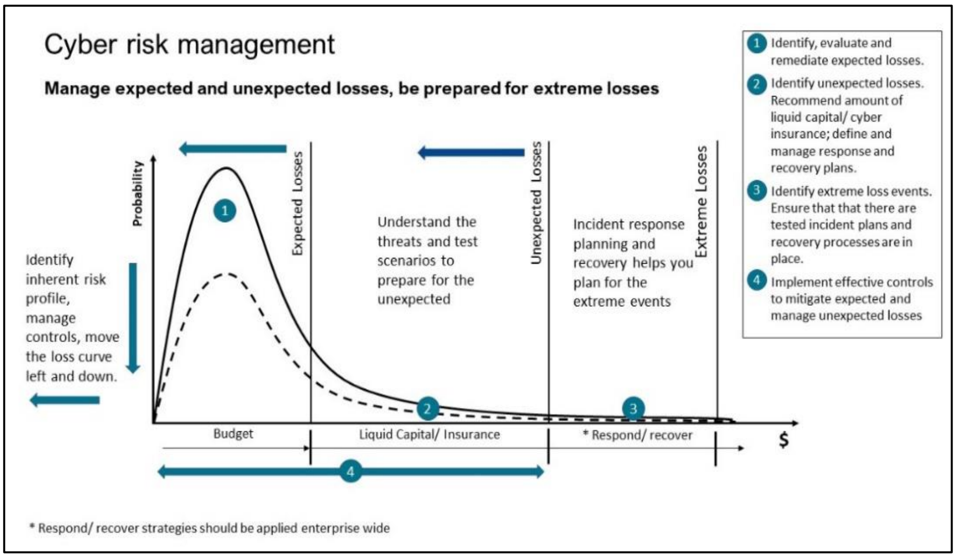

Cyber risk management
Manage expected and unexpected losses, be prepared for extreme losses
Probability
1
Expected Losses
Understand the threats and test scenarios to prepare for the unexpected
Unexpected Losses
Incident response planning and recovery helps you plan for the extreme events
Extreme Losses
Identify inherent risk profile, manage controls, move the loss curve left and down.
2
3
Budget
Liquid Capital/ Insurance
* Respond/ recover
$
4
1 Identify, evaluate and remediate expected losses.
2 Identify unexpected losses. Recommend amount of liquid capital/ cyber insurance; define and manage response and recovery plans.
3 Identify extreme loss events. Ensure that that there are tested incident plans and recovery processes are in place.
4 Implement effective controls to mitigate expected and manage unexpected losses
* Respond/ recover strategies should be applied enterprise wide

Figure 1: Risk Management. Expected, unexpected and extreme loss

The aim of risk management, the adoption of FISMA and the RMF is to reduce the impact of expected and unexpected losses, using an organization's controls. Using appropriate preventative, detective, or corrective controls to reduce the impact of the events, and manage residual risk aligned with their risk appetite. The organization should then adopt the controls in *NIST SP 800-53R5*, *NIST SP*

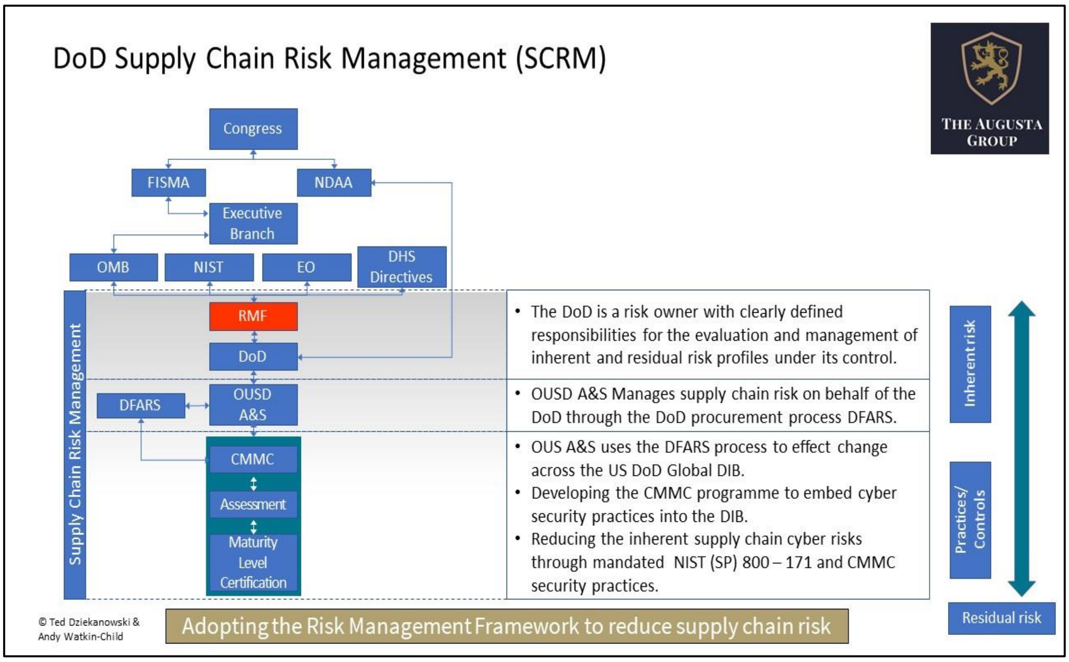
800-171R2, and the DoD *CMMC program.* This alignment will *determine* an organization's risk profile. The goal is to keep the area under the curve both to the left and reduce the peak in a manner that is manageable and understood (Figure 1).

If an organization does not implement an appropriate Risk Management Framework (RMF), it will be unable to fulfill the requirements of FISMA. The consequences of not following the RMF as required by FISMA and described in NIST SP 800-37R2 will include:

1. There will be no understanding, definition, or qualification of the risks affecting an organization.
2. The effectiveness of controls at managing cyber cannot be assessed.
3. The economic costs associated with the application of controls cannot be calculated.

An organization not aligning risk management with its strategic objectives and operations will be unable to apply the appropriate controls to manage cyber risk. FISMA (2014), the Office of Management and Budget (OMB) circular A-130, and NIST SP 800-37R2 are important in this regard. FISMA and OMB Circular A-130 ('*Managing Information as a Strategic Resource*') define the lens through which cyber security is regulated in the U.S. NIST SP 800-37R2 defines the mechanism for the implementation of the RMF, adopted by the DoD. Together they regulate, enforce, and define the requirements for an enterprise-wide risk management program to manage cybersecurity.

Figure 2 is the relationship between Congress, FISMA, the OMB, and the DoD for risk management, oversight, and assurance. FISMA legislates an enterprise-wide risk management program and system for all Federal agencies overseen by OMB. FISMA drives the alignment of a risk management strategy to mission and business objectives, with controls to mitigate risk and ensure adequate reporting of their continued effectiveness. FISMA has significant implications for all Federal Government Agencies to prioritize resources to mitigate risk, where there is a high impact on mission and business objectives and regard to future funding.



DoD Supply Chain Risk Management (SCRM)

- The DoD is a risk owner with clearly defined responsibilities for the evaluation and management of inherent and residual risk profiles under its control.
- OUSD A&S Manages supply chain risk on behalf of the DoD through the DoD procurement process DFARS.
- OUS A&S uses the DFARS process to effect change across the US DoD Global DIB.
- Developing the CMMC programme to embed cyber security practices into the DIB.
- Reducing the inherent supply chain cyber risks through mandated NIST (SP) 800 – 171 and CMMC security practices.

© Ted Dziekanowski & Andy Watkin-Child

Adopting the Risk Management Framework to reduce supply chain risk

Figure 2: The relationship between Congress, FISMA, OMB and the RMF

As a risk owner, the DoD has operationalized its requirements to comply with FISMA and OMB A-130 to deploy risk management. The RMF (*NIST SP 800-37R2*), DoDI 8500.01[18] (*Cybersecurity*), DoD 8510.01 (*Risk Management Framework for DoD Information Technology (IT)*), DoDI 5000.90 (*Cybersecurity for Acquisition Decision Authorities and Program Managers*), and DoDI 5000.83[19] (*Technology and Program Protection to Maintain Technological Advantage*) instructions. DoDI 5000.90 sets out the cybersecurity and risk management requirements for acquisition decision authorities and program managers for DoD IT systems across its procurement lifecycle. DoDI 5000.53 provides the procedures for science and technology managers and engineers to manage system security and cybersecurity technical risks. The CMMC program implements oversight and assurance of *Defense Federal Acquisition*

Supplement (DFARS) 252.204-7012, 7019, 7020, and 7021. Requiring the use of the *NIST SP 800 -171R2*[20] cybersecurity controls framework, with additional controls added in line with the maturity level agreed for a given contract.

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.

The role of FISMA and its applicability to Federal Agencies and their contractors requires them to implement information security protection in line with risk.

DoD 8510.01 (updated December 2020) is an important document for the DoD, figure 3 demonstrates the regulatory architecture which feeds the DoDI. DoDI 8510.01 sets out the requirement for the adoption of the Risk Management Framework (RMF) and transition from Defense Information Assurance Certification and Accreditation Process (DICAP). In response to FISMA and the Office of Management and Budgets (OMB) requirements to implement information security standards to Federal information systems (*40 U.S. Code § 11331 - Responsibilities for Federal information systems standards*). DoDI 8510.01 sets out the roles and responsibilities for the implementation of the RMF by the DoD including Acquisition and Sustainment, Research and Engineering, Developmental Test and Evaluation, DoD and OSD Component Heads, Defense Information Systems Agency (DISA), National Security Agency (NSA) and U.S. Space Command. It establishes the RMF and associated cybersecurity policies and assigns the responsibilities for executing and maintaining the RMF. DoDi 8510.01 replaces DIACAP and manages the life-cycle cybersecurity risk to DoD IT. The DoD has mandated the operationalisation of DoDi 8510.01 across all branches of the DoD. In this paper we outline the application of the RMF by the U.S. Air Force, through their instruction 17 - 101 (*Risk Management Framework (RMF) for Air Force Information technology*, February 2020).

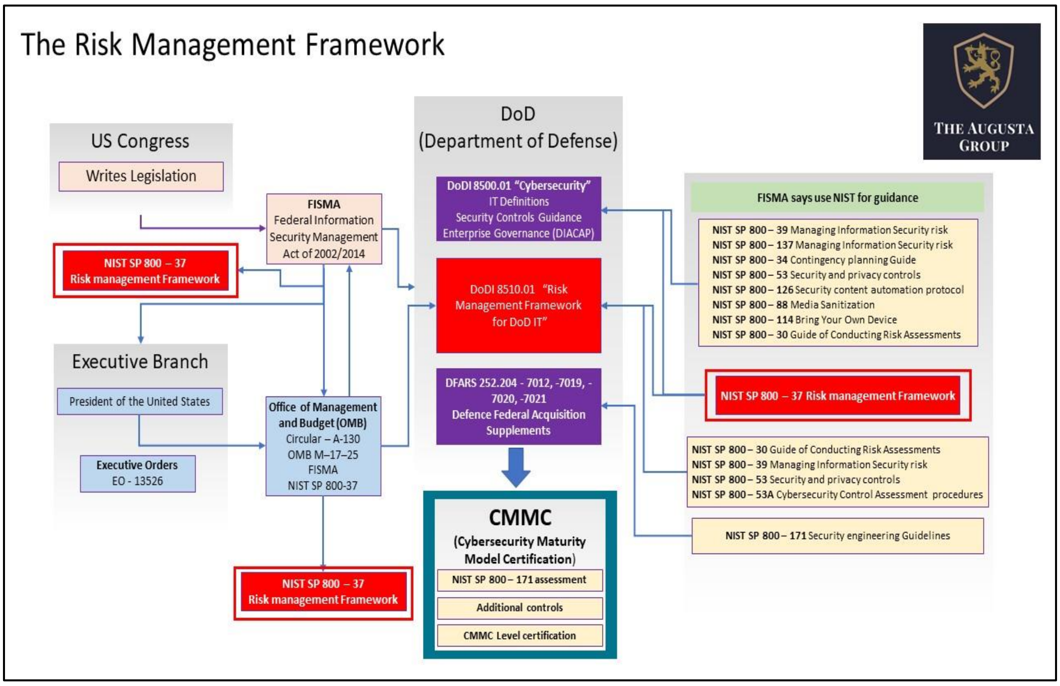

The Risk Management Framework
THE AUGUSTA GROUP
US Congress
Writes Legislation
FISMA
Federal Information Security Management Act of 2002/2014
NIST SP 800 – 37 Risk management Framework
Executive Branch
President of the United States
Executive Orders EO - 13526
Office of Management and Budget (OMB)
Circular – A-130
OMB M–17–25
FISMA
NIST SP 800-37
NIST SP 800 – 37 Risk management Framework
DoD (Department of Defense)
DoDI 8500.01 "Cybersecurity"
IT Definitions
Security Controls Guidance
Enterprise Governance (DIACAP)
DoDI 8510.01 "Risk Management Framework for DoD IT"
DFARS 252.204 - 7012, -7019, -7020, -7021
Defence Federal Acquisition Supplements
CMMC
(Cybersecurity Maturity Model Certification)
NIST SP 800 – 171 assessment
Additional controls
CMMC Level certification
FISMA says use NIST for guidance
NIST SP 800 – 39 Managing Information Security risk
NIST SP 800 – 137 Managing Information Security risk
NIST SP 800 – 34 Contingency planning Guide
NIST SP 800 – 53 Security and privacy controls
NIST SP 800 – 126 Security content automation protocol
NIST SP 800 – 88 Media Sanitization
NIST SP 800 – 114 Bring Your Own Device
NIST SP 800 – 30 Guide of Conducting Risk Assessments
NIST SP 800 – 37 Risk management Framework
NIST SP 800 – 30 Guide of Conducting Risk Assessments
NIST SP 800 – 39 Managing Information Security risk
NIST SP 800 – 53 Security and privacy controls
NIST SP 800 – 53A Cybersecurity Control Assessment procedures
NIST SP 800 – 171 Security engineering Guidelines

Figure 3: The relationship between Congress, FISMA, the Executive Branch, OMB, NIST and the DoDs Risk Management Framework (RMF)

The scope of coverage of the DoD RMF program (incorporating US Air Forces AFI 17-101) is broad and complex. Ranging from individual hardware and software products, standalone systems and larger computing environments, enclave, and networks. Identified in Figure X below.

Not all IT products, services and PIT systems are covered fully under the RMF process, as some of these systems must be securely configured in accordance with applicable DoD policies and security controls, undergoing special assessment of their functional and security-related capabilities and deficiencies.

By way of example, we will discuss Air Force Instruction AFI 17 - 101 (February 2020) as the most up to date RMF adopted by the UD DoD, utilizing NIST SP 800-37-R2.

Compliance to Air Force Instruction (AFI) 17 - 101, Risk Management Framework (RMF) for Air Force Information technology is mandatory. AFI provides the instructions for the implementation of the Risk Management Framework (RMF) for Air Force (AF) Information technology (IT), in accordance with AFPD 17 - 1 (*Information Dominance Governance and Management)* and AFI 17 - 130 (*Air Force Cybersecurity Program Management).* The purpose of AFI 17 – 101 is to,

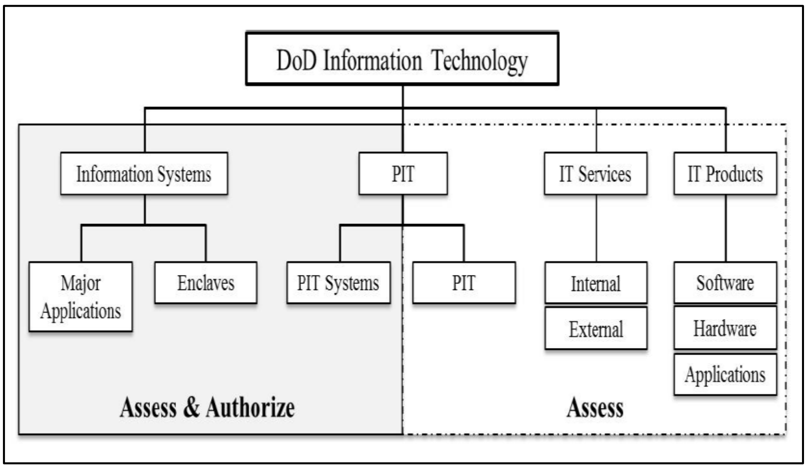


Figure 4: Scope of DoD information technology

- Incorporate strategy, policy, awareness/training, assessment, continuous monitoring, authorization, implementation, and remediation.
- Align with Secretary of the Air Force/ Deputy Chief Information Officer (SAF/CN) strategic goals and objectives key concept of cybersecurity that works which requires robust risk assessment and management.
- Encompasses life cycle risk management to determine and manage the residual cybersecurity risk to the AF created by the vulnerabilities and threats associated with objectives in military, intelligence, and business operations.
- Implement privacy and security controls based on the assessed and mitigated residual risk. The controls align with Department of Defense Instruction (DoDI) 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT) and are documented in the RMF security authorization package for AF IT.

AFI 17 - 101 is applicable to

- Information Technology supporting research, development, test, and evaluation (T&E), and DoD-controlled IT operated by a contractor or other entity on behalf of the DoD. AF IT, information systems (major applications and enclaves), platform information technology (PIT) (PIT systems, PIT subsystems, and PIT products), IT services (internal & external), IT products (software, hardware, and applications) and boundary requirements for assess and authorize and assess only (see Chapter 5).
- Risk management authorities for special access programs are executed via AFI 17-101, or where they apply, more restrictive policies
- AFI 17 - 101 does not apply to the protection of sensitive compartmented information systems (IS) or intelligence, surveillance, reconnaissance mission and mission support systems.
- Authority for AF space systems rests with AF Space Command as delegated by United States Strategic Command.

- For IT not centrally managed or that has yet to be assigned an authorizing official (AO), the unit responsible for ownership or operation of the IT shall assign duties for the minimum RMF relevant roles (see Table 3.1) required to comply with RMF. The duties shall include the roles and responsibilities for reporting, oversight, and risk management to the AF.

The objectives of AFI 17 - 101 include

- To provide a disciplined and structured process to perform AF IT security and risk management activities and to integrate those activities into the system development life cycle. The RMF provides a dynamic approach to risk management that effectively manages mission and cybersecurity risks in a diverse environment of complex, evolving, and sophisticated cyber threats and vulnerabilities.
- To ensure AF IT assets are assessed for cybersecurity risk. Discovered weaknesses are documented in a plan of action and milestones (POA&M) to mitigate residual risk. An AO, identified at Table 3.1, who is supported by an RMF team, accepts the risk for his/her area of responsibility, in accordance with DoDI 8510.01, and the Air Force RMF Knowledge Service.

The DoD has developed risk policy as described by DoDI 8510.01 *(Managing Information Security Risk)*, aligned with NIST SP 800 - 39. Integrating the RMF across all phases of the IT Life cycle, spanning logical and organizational entities. Integrating cyber-risk assessment and decision making across all tiers of DoD organizational decision, through business process down to Information and Pit Systems as described in Figure 5, the DoD governance for the Risk management Framework (RMF)

Tier 1 – Organization. Is the Office of the Secretary of Defense, which addresses risk management at an enterprise level. Under which the Senior Information Security Officer (DoD CISO), Risk Executive function, Cybersecurity Architecture RMF TAG form and deliver the DoDs strategic executive risk management capabilities for the delivery, oversight, and assurance of risk management for the DoD.

Tier 2 – Mission/ Business processes. Define the accountable and responsible functions within the DoD and the roles and responsibilities for the delivery of risk management strategy under FISMA. Including those of the relevant Senior Information Security Officer (SISO), (Principle) Authorizing Officials (PAO), DoD Component CIOs, Warfighting Mission Area (MA), Business Mission Area (BMA), Enterprise Information Environment Mission Area (EIEMA) and System Managers (SM).

Tier 3 – IS and Pit Systems.

Identifies the responsible roles and responsibilities for delivering risk management, oversight, and assurance of FISMA. Ensuring that FISMA regulations and RFM tasks are initiated, completed and appropriate documentation is assigned to Information and PIT systems. That a system security program is in place and actively managed, system security plans (SSP) are developed, maintained, and tracked and AO authorization decisions are enforced.

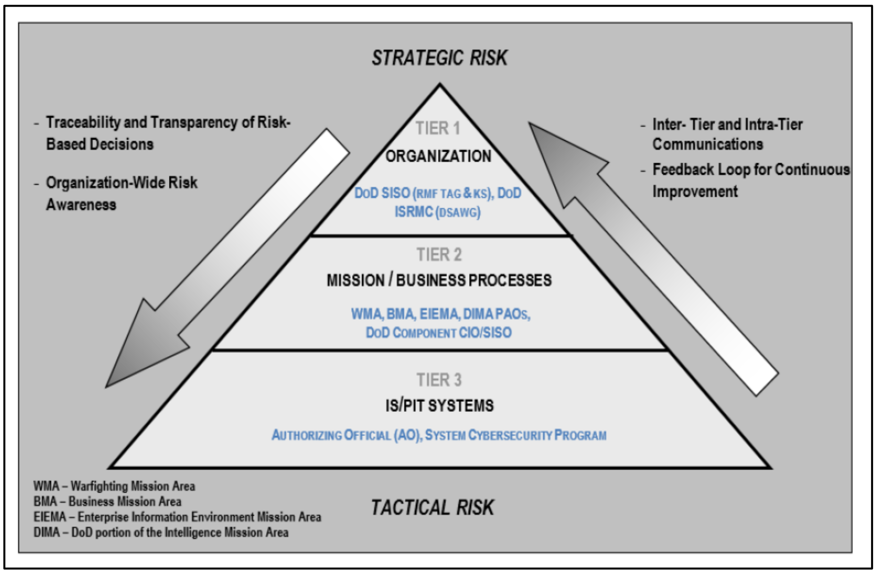

STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
TIER 1
ORGANIZATION
DoD SISO (RMF TAG & KS), DoD ISRMC (DSAWG)
TIER 2
MISSION / BUSINESS PROCESSES
WMA, BMA, EIEMA, DIMA PAOs, DoD Component CIO/SISO
TIER 3
IS/PIT SYSTEMS
Authorizing Official (AO), System Cybersecurity Program
- Inter- Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
WMA – Warfighting Mission Area
BMA – Business Mission Area
EIEMA – Enterprise Information Environment Mission Area
DIMA – DoD portion of the Intelligence Mission Area
TACTICAL RISK

Figure 5: DoD Risk Management Framework Governance

The Risk management methodology governed under AFI 17 - 101 follows the specific guidance provided by NIST SP 800-37R2 (*Risk Management Framework for Information Systems and Organizations*). It follows a process which is iterative throughout the entire lifecycle for IT IAW DoDI 5000.02 and the DoD Program Manager's *Guidebook for Integrating the Cybersecurity Risk*

Management Framework (RMF) into the System Acquisition Lifecycle. AFI 17 - 101 describes 7 risk management steps that include Prepare, Categorize, Select, Implement, Access, Authorize and Monitor (Figure 6).

Step 1 – Prepare. The purpose of Prepare step of the RMF is to identify essential activities of organization, mission, and business processes. The program manager/ RMF team is required to fill out the ITCSC during this step to identify and prepare for the management of cybersecurity and privacy risks.

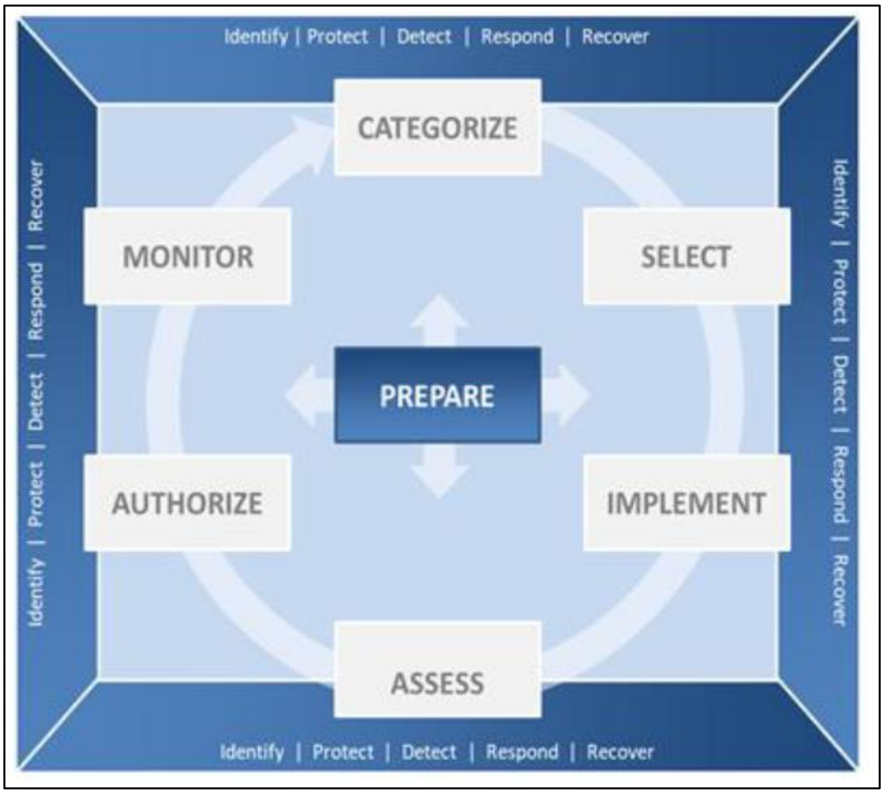

Identify | Protect | Detect | Respond | Recover
CATEGORIZE
MONITOR
SELECT
PREPARE
AUTHORIZE
IMPLEMENT
ASSESS
Identify | Protect | Detect | Respond | Recover
Identify | Protect | Detect | Respond | Recover
Identify | Protect | Detect | Respond | Recover

Figure 6: Risk Management lifecycle

Step 2 – Categorize the system referencing DoDI 8510.01, CNSSI No.1253 (*Security Categorization and Control Selection for National Security System)*, NIST SP 800-53R5 (*Security and Privacy Controls for Federal Information Systems and Organizations – now R5),* NIST SP 800 – 60 (*Guide for Mapping Types of Information and Information Systems to Security Categories*, and the DoD and AF RMF KS (OPR: PM/ISO). Documenting the potential impact resulting from the loss of confidentiality, integrity, and availability in the event of a security breach.

Step 3 - Select security controls referencing References DoDI 8510.01, CNSSI No.1253, NIST SP 800-30, NIST SP 800-53R5, and the DoD and AF RMF KS (OPR: PM/ISO). Common controls are identified following a risk assessment conducted by Tier 1 and Tier 2 entities (see Figure 5 above and DoDi 8510.01) and selected from the DoDs Knowledge System (KS). Using the security control baseline identified as part of the IT categorization step.

Controls should be tailored as required and every selected control must be accounted for either by the organization or the Information Security Officer. If a control is added or de-selected from the baseline (i.e. tagged as not applicable), then a risk-based rationale must be documented in the security plan and POA&M.

An Information Security Continuous Monitoring (ISCM) strategy should be developed for the continuous monitoring of the effectiveness of the security controls employed within or inherited by the system and monitoring any proposed or actual changes to the system and its operating environment. The Authorizing Officer (AO) will review and approve the security plan and system-level continuous monitoring strategy submitted by the Program Manager or Information Security Officer.

Step 4 – Implement Security Controls referencing DoDI 8510.01, NIST SP 800-53R5, applicable security technical implementation guides, security requirements guide, and the DoD and AF RMF KS. (OPR: PM/ISO).

Step 5 – Assess security controls referencing DoDI 8510.01, NIST SP 800-30, NIST SP 800-53R5, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, applicable Security Technical Implementation Guide, Security Requirements Guides, and the DoD and AF RMF KS. Use DoDI 8510.01, enclosure 6 instructions for details for assessing security controls (OPR: SCA).

Step 6 – Authorize system after reviewing the security authorization documentation, the AO formally accepts or rejects risk by authorizing the IT through an interim authority to test, authorization to operate, authorization to operate with conditions, or a denial of authorization to operate. References DoDI 8510.01, enclosure 6 (OPR: AO/AODR).

AOs will issue an interim authority to test, authorization to operate, or an authorization to operate with conditions for any risk determined not to be "Very High" or "High".

Authorization to operate with conditions for unmitigated "Very High" or "High" risk.

- The Secretary of the Airforce (AF) is the only Air Force authority that may grant an AO the approval to issue an Authorization to Operate (ATO) with "Very High" or "High" risk/ (formerly known as CAT I) non-compliant security controls that cannot be corrected or mitigated immediately, but where the overall risk is acceptable due to mission criticality. Delegation below the SAF/CN is not authorized. IT with "Very High" or "High" risk, which are authorized by other DoD Components connecting to the AF information networks require Component CIO approval, and a joint system requires DoD CIO approval.
- IT with unmitigated "Very High" or "High" risk non-compliant security controls must follow the Very High/High Package Submission Guide requiring the Authorizing Official to submit completed packages to the SAF/CN for approval prior to making an authorization decision. (T-0)
- For "Very High" or "High" risk authorizations, the authorization to operate with conditions will be issued for up to 1 year. When a 1-year authorization to operate with conditions is issued, the authorization to operate with conditions must specify a review period that is within 6 months of the authorization termination date (ATD). (T-1)

Denial of Authorization to Operate

- If risk is determined to be unacceptable when compared to the mission assurance requirement, the authorizing official, in collaboration with all program stakeholders, will issue a denial of authorization to operate. If the system is already operational, the responsible AO will issue a denial of authorization to operate, and operation of the system will cease immediately. Network connections will be immediately terminated for any system that is issued a denial of authorization to operate.

Step 7 – Monitor Security Controls References DoDI 8510.01 and NIST SP 800-137, *Information Security Continuous Monitoring* (ISCM) *for Federal Information Systems and Organizations* (OPR: PM/ISO and ISSM).

- DoDI 8510.01 and the DoD RMF KS for Continuous Monitoring provides a detailed framework on continuous monitoring, which should be used to augment the continuous monitoring program for the IT.
- The objective of an Information Security Continuous Monitoring (ISCM) program is to determine if the complete set of planned, required, and deployed security controls within a system or inherited by the system continue to be effective over time in light of inevitable changes.
- Documenting proposed or actual changes to a system or its environment of operation and subsequently assessing the potential impact those changes may have on the security state of the system or the organization is an important aspect of security control monitoring.
- All implemented security controls, including management and operational controls, must be regularly assessed for effectiveness, even if monitoring them is not easily automated.

- Authorizing Officials must consider how ISCM will be implemented organization wide as one of the key components of the security life cycle represented by the RMF.
- Individual system-level ISCM strategies must align with the organization's broader ISCM strategy.
- If the change results in a new "Very High" or "High" risk non-compliant security control(s) that can be corrected within 30 days or a new Moderate risk that can be corrected/satisfactorily mitigated within 90 days, the system can continue to operate under the existing authorization decision and connection approval as referenced in DoDI 8510.01.

Integrating the RMF into the Defense Acquisition Management System.

The Air Force RMF AFI 17 - 101 is closely aligned to the DoDs own RMF defined under DoDI 8510.01, that is turn is designed to be complementary to, and supportive of, DoD's acquisition management system activities, milestones, and phases. RMF activities should be initiated as early as possible in the DoD acquisition process to increase security and decrease cost. Requirement's development, procurement, and T&E processes should be considered when applying the RMF to the acquisition of DoD IT. Threats to these systems should be designated consistent with the most severe risk to any individual component or subcomponent for consideration of requirements, acquisition, and testing and evaluation.

This is demonstrated by the release of DoDI 5000.90 "Cybersecurity for Acquisition Decision Authorities and Program Managers," on the 31st of December 2020. Setting out the foundations for cybersecurity risk-based decision making within the Defense Acquisition System using the RMF. DoDI 5000.90 is a risk-based approach for cybersecurity oversight and assurance within the DAS and establishes policy, assigns responsibilities, and prescribes the procedures for managing cybersecurity risk by program Decision Authorities (DA) and Program Managers (PM) in the DoD acquisition process. Requiring the assessment and management of cyber-risk across the defense acquisition lifecycle. Establishing policy, standards, and guidance to qualify and quantify cybersecurity risks across acquisition programs arising from adversaries targeting suppliers and supply chains.

Cybersecurity Foundations in the Defense Acquisition System ("DAS")

DAS is a core capability in assuring that the DoD is equipped to win military operations in all warfighting domains. It encompassed the DoD's Adaptive Acquisition Framework (AAF) applied to the acquisition of weapon systems and processes ranging from service, major capability, urgent capability, software, and business system and R&D acquisition processes. This is for the procurement of platforms, weapon systems, and the DIB,

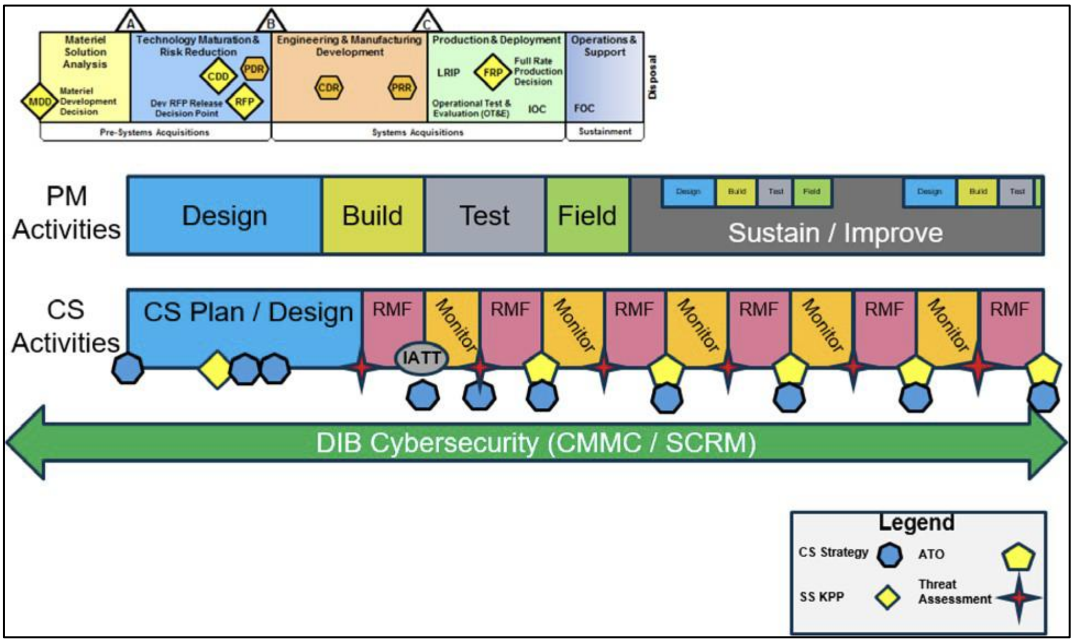


Figure 7: DAS Cybersecurity planning and execution

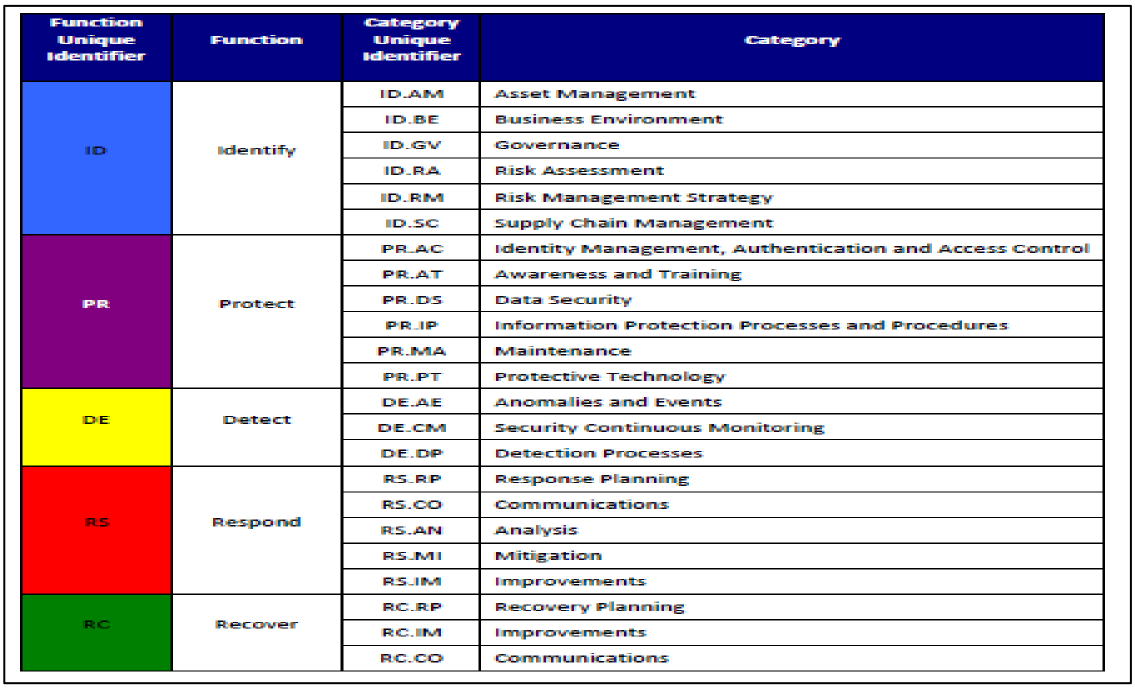
ensuring that cyber-risks and cybersecurity are appropriately assessed, resourced, and mitigated within the DoDs supply chain.

"Provides a clear focus on the role of acquisition program managers and decision authorities as coordinators and overseers of all aspects of cybersecurity in acquisition programs."

Cybersecurity crosses all pathways within the AAF. Embedding cybersecurity into all aspects of the DAS is critical for securing DoD weapon systems and their DIB. The DAS enables procurement DAs and PMs to reinforce cybersecurity through the deployment and continual reinforcement of cybersecurity risk management practices. They are making risk-based procurement decisions through existing procurement processes, with the potential of refusing to award the DIB contracts based on the adoption of poor cyber-risk management. CMMC/ SCRM are referenced by DoDI 5000.90 as frameworks to be adopted across the product design, build, test, field and execution lifecycle.

Cybersecurity Framework (CSF) profiles - Identify, Defend, Protect, Respond, Recover.

Figure 6 identifies not only the different steps in the RMF, but points to the use of the NIST Cybersecurity Framework profile[21] and the adoption of cybersecurity practices aligned to the NIST CSF categories of Identify, Defend, Protect, Respond and Recover. NIST created the Cybersecurity Framework (NIST CSF) as a comprehensive standard, guideline, and best practice to help organizations improve their management of cybersecurity risk. Figure 8 details typical CSF functions and categories. It was designed to be flexible enough to integrate with the existing security processes within any organization, in any industry. It is mapped to other NIST frameworks such as NIST SP 800 - 171.



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Management
PR	Protect	PR.AC	Identity Management, Authentication and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figure 8: Indicative NIST Cybersecurity Framework Profile

The NIST Cybersecurity framework Manufacturing profile, released in October 2020 (NISTIR 8183[21]) has been tailored by NIST for the manufacturing industry. It addresses gaps in NIST SP 800 - 171, namely asset management governance, the business environment, risk management and supply chain management. Key practices required by an organization's board and corporate regulators to demonstrate implementation of cyber-SCRM. It is consistent with NIST CSF aligning practices to Identify, Protect, Detect, Respond and Recover from cyber incidents, and practices to close the gaps with NIST SP 800 – 171R2 and SP 800 - 53R5. Removing duplication of effort with NIST SP 800 – 171R2 security practices which are mapped to the SCF.

Conclusion

The United States Government addressed C-SCRM when Congress passed FISMA in 2002, adopted the RMF, and established regulation by the OMB under circular A-130. Both FISMA and OMB A-130 form the foundation of US Federal Government cyber risk management.

In response, the DoD has mandated its branches to adopt the RMF for cybersecurity risk management using DoDI 8510.01. DoDI 8510.01 implements FISMA, OMB A-130, and NIST standards to manage the cybersecurity risk of its information systems. The risk management lifecycle in figure six shows the cybersecurity risk management process, for the identification, and categorization of threats and associated risks to DoD systems. The identification, documentation, and assessment of the controls used to mitigate those risks and the authorization mechanisms through the ATO process for authorizing the use of systems based upon appropriate risk management. Risks can only be exempt by personnel working for the DoD, in line with agreed mission and business objectives, as demonstrated by the USAF in AF 17 - 101.

FISMA and the RMF have been integral to US cyber regulation and cybersecurity risk management for almost 20 years. This period has seen a dramatic increase in the complexity, severity, and several cyber-attacks across Federal Government and US companies resulting in the theft and destruction of IP related to national security and corporate competitive advantage. NIST developed cybersecurity framework (CSF) profiles to enable a flexible approach to cybersecurity controls based upon mission and business objectives. If applied as part of NIST SP 800 - 37R2, they provide a viable tool to mitigate risk.

Well-informed risk-based decisions are necessary to balance the benefits gained from the operation and use of information systems. Managing information security risk brings together the best collective judgments of individuals and groups within organizations responsible for strategic planning, oversight, management, and day-to-day operations. This adoption provides the necessary risk response to protect the mission-critical and business functions of those organizations. FISMA is an important regulation, applicable and enforceable across the Federal Government. If applied with appropriate oversight, it can be used to identify, quantify, and manage cybersecurity risk. FISMA addresses the application of C-SCRM, enabling a risk-based approach for the management of cybersecurity.

Options

Option 1: Do nothing. If Federal government continues its current path, whereby it struggles to implement the full intent of FISMA, in part due to the lack of consequences dating back to 2002 and 2014. The result will be the on-going exfiltration of data, an increase in the financial impact of cyber-attacks, and no assurance of the security posture of the US supply chain. The benefit of this approach is no new regulatory requirements are foisted upon Federal Agencies and suppliers of the U.S. Government.

Option 2: Enforce current FISMA regulation to provide oversight and assurance by Federal Agencies. Putting in place the appropriate standards for assessment and enforcement to incentivize Federal Agencies manage supply chain risk. Enabling the Department of Homeland Security (DHS) oversight and assure critical infrastructure. So that Federal Government is better informed and capable of making risk-based decisions and providing greater oversight of supply chain risk management by Federal Government. However, option 2 would require a significant number of assessors, and increase FISMA compliance costs on domestic and international businesses.

Option 3: Re-imagine FISMA and enforce it. Society has been transformed over the past 10 years with the introduction and maturity of platforms such as Cloud, Blockchain, AI, Machine Learning and Big

Data. Society now relies on information; it is the most important commodity which we own as individuals and organizations, across both the public and private sectors. Systems now are much more dynamic utilizing compute, network and storage making the concept of a conventional system seem far less important. Infrastructure as code, serverless computing (Function as a Service) and containerization also make creating and maintaining a tradition System Security Plan with the requisite assessment and authorization even more challenging.

Therefore, any changes made to FISMA should now be focused upon information 'types'. The 'types' of information require the information owner to establish its value and the level of protection which should be applied to it, based upon a risk assessment by proper classification and categorization, regardless the physical infrastructure upon which it may resides.

The unique nature of information types managed by an organization, its risk profile and security posture support the creation and use of unique CyberSecurity Framework (CSF) profiles, as a contractual enforcement mechanism. A CSF can be tailored by an organization to satisfy its mission and business objectives to mitigate the risks associated with the loss or damage to its data. As referenced by NIST SP 800-37R2 (Prepare step 1, task 6), bringing the residual risk to an acceptable level based on the risk tolerance of the organization.

Given the nearly impossible task for Federal government to monitor everything, a more efficient use of limited resources would be to focus on protection of information types. That have a high target value to an adversary and where the impact of loss or compromise would cause significant harm to the United States.

To prescribe a level of protection for information that would be acceptable globally it may be time to adapt a mechanism already that was once used to create an internationally recognized standard for certification and accreditation, called Common Criteria.

Common Criteria define protection requirements in a protection profile and detailed the level of security and assurance which can be assessed by a partner nation for given hardware and software. The levels of assurance include functionally tested, structurally tested, methodically tested, and checked, Semi-formally designed and tested**, s**emi-formally verified design and tested and formally verified design and tested. By adapting protection profiles for information types, controls that provide assurance of adequate protection can be internationally agreed, allowing for the free movement of data globally. Solving third party vendor issues around supply chain risk management. The controls identified in protection profiles can be mapped into Cyber Security Framework Profiles for a specific contracts where the CSF profile can be further tailored to meet specific organizational requirements.

FISMA needs to be reimagined and regulated to address Federal Governments (by extension State, Local and Tribal Governments) poor implementation of cybersecurity risk management. As highlighted by the Senate Homeland security and Government affairs committee in August 2021[23], and the need to address international cyber, data and information standards and reciprocity as illustrated by the recent White House announcement following the Quad leaders Summit in September 2021[24].

Under FISMA it is our belief that both Federal agencies and contractors to Federal Agencies must implement the RMF to identify and provide information security protections commensurate with the risk and the magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of Federal information. We feel that this document informs both the public and private sector of FISMA requirements to ensure that agencies fulfil FISMA's primary legislative objective to secure federal networks.

About the authors and contributors

Andy Watkin-Child (Author) is a 20-year veteran of cyber security, risk management and technology. He has held international leadership positions in 1st and 2nd Lines of Defence (LoD) for cyber security, cyber-risk management, operational risk, and technology. For companies across Engineering and Manufacturing, Financial Services and Publishing and Media. Working with leadership teams of companies with balance sheets over €1TRN. He is an experienced member of management boards, global risk leadership teams, cyber security, operational risk and GDPR committees.

He holds Royal Charters in Security (CSyP), recognised by the UK Centre for the Protection of National Infrastructure (CPNI) and Engineering (CEng). He has a place on the UKs Register of Chartered Security Professionals. He is a member of the Board of the Security Institute (MSyI), the largest UK members only security trade association, he is a Freeman of the Worshipful Company of Security Professionals (WCoSP) and a Freeman of the City of London. He is a counsel appointed expert witness who specialises in cyber and risk management a Practicing Associate of the Academy of Experts (AMAE) and advised the Information Commissionaires Office (ICO) on high profile GDPR cases. He is a member of the US CMMC Accreditation Body (CMMC-AB) standards working group, developing the CMMC assessment methodology. Chair of Team Defence Information (TDI) CMMC working group working with UK defence trade associations in support of the deployment of CMMC into the UK DIB.

Andy is the Founding Partner of the Augusta Group an independent UU based cyber-risk management advisory firm, supporting organisations deliver cyber-risk management, education and cyber regulatory programmes. www.augustagrp.com

https://www.linkedin.com/in/andywatkinchild/

Ted Dziekanowski (Author) is a veteran of cybersecurity with over 40 years' experience of the design, delivery, oversight and assurance of cybersecurity and risk management systems. Ted's area of expertise is the management of risk in Information Technology developed over the years. He is an experienced systems Auditor and Integrator giving him a unique insight as to the challenges associated with developing an eGRC program that satisfies the compliance requirements faced by organizations of all types and sizes.

He is an internationally recognised cybersecurity, risk management and Information system auditor. A highly respected security trainer, authorized to train ISACA CISA, CISM, CRISC, ISC2 CAP, CCSP, and CISSP. He holds DoD secret clearance and has taught causes for a broad range of public and private sector (available on request)

https://www.linkedin.com/in/tdziekanowski/

Jason Spezzano (contributor) is an experienced cybersecurity services delivery leader and consultant with over 25 years of experience. Specialties include risk management, compliance, and cybersecurity operations supporting DoD, Federal and Intelligence Agencies. Jason is currently the Senior Director of Cybersecurity at Grammatech, a leading developer of software-assurance tools and advanced cybersecurity solutions, as well as a Senior cybersecurity consultant focused on Governance, Risk Management and Compliance (GRC) using information security frameworks established by the National Institute of Standards and Technology (NIST).

Jason is also a Fellow with the Cybersecurity Forum Initiative (CSFI) and a former Major in the United States Marine Corps.

https://www.linkedin.com/in/jason-spezzano-aaa862b/

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. Risk Management Framework (NIST SP 800 - 37R2): https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
9. Office of Management and Budget Circular A 130: https://www.cio.gov/policies-and-priorities/circular-a-130/
10. US Department of Defence (DoD) RMF instruction DoDi 8510.01: https://www.dodea.edu/Offices/PolicyAndLegislation/upload/DoDEA-AI-8510-01-Risk-Management-Framework.pdf
11. US Department of Defence (DoD) RMF instruction DoDi 5000.90: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500090p.PDF?ver=MIG3uLnzXl31QcvXJTZ5uA%3D%3D
12. DFARS 252.204-7012: https://www.law.cornell.edu/cfr/text/48/252.204-7012
13. U.S. Air Force Instruction (AFI) 17-101, Risk management framework (RMF) for Air Force - Information Technology (IT): https://static.e-publishing.af.mil/production/1/saf_cn/publication/afi17-101/afi17-101.pdf
14. World Economic Forum: Principles for board governance of cyber-risk (March 2021) http://www3.weforum.org/docs/WEF_Cyber_Risk_Corporate_Governance_2021.pdf
15. NATO recognises cyber a security domain: https://www.nato.int/cps/en/natohq/topics_78170.htm#:~:text=On%2014%20June%202016%2C%20Allied,in%20accordance%20with%20international%20law.
16. US DOD Office of Small Business: https://www.acq.osd.mil/news/featured/small-businesses-key-to-nations-defense.html
17. The cost of a cyber-attack: https://www.insurancebusinessmag.com/us/news/cyber/global-cyber-insurance-pricing-spikes-32--report-259795.aspx
18. US Department of Defence (DoD) RMF instruction DoDi 8500.01: https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/850001_2014.pdf
19. US Department of Defence (DoD) RMF instruction DoDi 5000.83: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500083p.pdf
20. NIST SP 800 - 171R2: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
21. NIST Manufacturing cybersecurity framework profile: https://csrc.nist.gov/News/2020/cybersecurity-framework-v1-1-manufacturing-profile#:~:text=This%20revision%20of%20the%20CSF,cybersecurity%20risk%2C%20vulnerability%20disclosure%2C%20system
22. Common Criteria: https://en.wikipedia.org/wiki/Common_Criteria
23. Homeland security committee on FISMA: https://www.hsgac.senate.gov/media/minority-media/new-bipartisan-portman-peters-report-shows-federal-agencies-cybersecurity-failures-leaving-americans-personal-information-at-risk
24. Whitehouse Quad leaders' Summit (Sept 2021): https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/fact-sheet-quad-leaders-summit/