



The Augusta Plan 3: Harmonising Cybersecurity And Risk Management Across Federal Agencies And Between The U.S And Its International Partners.

Leveraging Existing Regulatory Practices, Frameworks, And Standards To Deliver Harmonised Cybersecurity Risk Management.

September 2022

Andy Watkin-Child, Ted Dziekanowski

Introduction

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, securing the sovereignty of nations against hostile threat actors required a collective effort of nation states for the protection of national and international security. This paper sets out in brief an approach to harmonise cybersecurity risk management data security across Federal Agencies and between the U.S and its partners. To protect data critical to national security while providing appropriate oversight and addressing the sovereignty of partner nations.

The challenges associated with the harmonisation of international cybersecurity standards are not new. In the 1980s and early 1990s you had 3 different international standards, [ITSEC](#) – The European standard, [CTCPEC](#) – The Canadian standard and [TCSEC](#) – The [United States Department of Defense](#) standard. What we propose is the adaptation of the existing international standard called the 'Common Criteria for Information Technology Security Evaluation' ^{1, 2}. There already exists agreements that are used to assess the security of information systems and the systems that process and manage information system 'Common Criteria'. We propose re-purposing this standard to apply to harmonisation, evaluation and adoption of cybersecurity risk management regulation and agreeing CyberSecurity Framework (CSF) protection profiles for given information types based upon the potential low, medium, and high-risk impact associated with information types. Information types defined in for example NIST SP 800-60 (Guide for Mapping Types of Information and Information Systems to Security Categories). Applying the existing 'Common Criteria' standard to seek agreement and harmonisation of cybersecurity risk management regulation and CSF protection profiles between those existing participating partners (as a starting point). Partners currently include certificate producers and certificate consumers from the U.S, Australia, Austria, Canada, Czech Republic, Denmark, Ethiopia, Finland, France, Germany, Greece, Hungary, India, Indonesia, Israel, Italy, Japan, Malaysia, Netherlands, New Zealand, Norway, Pakistan, Poland, Qatar, Republic of Korean, Singapore, Slovak Republic, Spain, Sweden, Turkey, United Kingdom.

Adopting the 'common criteria' approach provides a solution that we believe leads to (1) the harmonisation of cybersecurity risk management regulation applied across Federal Government, and between the U.S and its partners. (2) the development of agreed 'baseline' CSF protection profiles for information types that are based upon an assessment of information risk. Creating 'baseline' CSF protection profiles for a given information type (National Security and Defense, Health, Personnel, energy, education, law enforcement, legal) focuses cybersecurity risk management on the most critical assets of both governments and organisations that is their data. CSF protection profiles can be used to provide a tool for contract negotiation, enabling buyers and sellers manage their cybersecurity expectations.

We are doing this today: *'Inadvertently the DoD DFARS/ CMMC program is an example where a cybersecurity standard (CSF Protection profile) has been applied to the*



information type of Controlled Unclassified Information (CUI). It has been applied without national or international agreement, harmonisation or an internationally agreed method of oversight and assurance.'

Background

U.S Federal government agencies and international partners are adopting cybersecurity risk management regulation at a significant pace. Regulation that is being applied to secure Federal Agencies directly (*Strengthening Americas Cybersecurity Act 2022*) or applied by agencies to improve national security (*DoD DFARS/ CMMC program*). U.S partner nations are also moving ahead with cybersecurity risk management regulations to secure critical infrastructure. Including for example the EU (*EU NIS 2.0 and DORA*), Australia (*Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022*) and India (CERT-In directives). The unintended consequences of the current approach include regulatory duplication; high compliance costs; no visible mechanism for national and international compliance oversight and assurance, plans to achieve high compliance requirements, and limited cybersecurity risk management resources. These compliance issues impact U.S national security, the security of partner nations and the national sovereignty of partner nations.

The Armed Services Committee and 2023 NDAA specifically raised concerns about the United Kingdom Ministry of Defence Industry Security Notification ISN 2021/03. The 2023 NDAA Highlights concerns regarding the Ministry of Defence illustrates the UKs cybersecurity standards and practices may not be adequate to those required under DFARS and the potential for other foreign governments to issue similar directives to their defense contractors. It is not unrealistic to assume that the issues faced by the UK are prevalent with other U.S Defence Department Partners, increasing the urgency and need for a comprehensive national and international solution for the harmonisation of cybersecurity risk management, frameworks, standards, and policies.

Fundamental issues

There are challenges implementing cybersecurity risk management across Federal Agencies, and between the U.S and its partners, namely

1. **Federal harmonisation** - Federal Agencies that create their own cybersecurity risk management regulations, frameworks and standards causes regulatory confusion, duplication and oversight and assurance challenges.
2. **International harmonisation** - U.S partners adopting differing cybersecurity risk management regulations and standards create conflicting requirements across national and international supply chains.
3. **Standards** - Federal Agencies and U.S. partners use different cybersecurity and risk management standards.
4. **Oversight and assurance** – There are no agreed mechanisms to oversight and assurance cybersecurity risk management compliance between the U.S and its partners. There is no consistency of compliance oversight.
5. **Resources** - There are not enough resources to implement, oversight and assure cybersecurity regulations nationally and internationally.
6. **Cost effective** - There needs to be a cost-effective solution to provide assurance, delivered through harmonised regulations and standards.
7. **National security** – U.S partner nations are not fully committed to meet existing U.S cybersecurity regulatory requirements (Armed Services Committee and NDAA 2023, above).

Addressing these issues

- a. **Regulatory harmonisation:** Using a *common criteria* like approach to harmonise cybersecurity regulations across Federal Agencies and between the U.S and its partners. Formalising a process for the creation, evaluation, authorisation, oversight and assurance of national and international cybersecurity regulation, that is aligned to the needs of nations, protects their sovereignty and is harmonised between the U.S and its partners. Another benefit of this approach would be to align common regulatory requirements, for example between the recent Securities and Exchange Commissions (SEC) cybersecurity risk management proposal, the EU directive EU NIS 2.0 and the proposed Digital Operational Resilience Act (DORA).
- b. **Common baseline cybersecurity protection profiles:** We propose using the 'Common criteria' method to create cybersecurity framework (CSF) protection profiles for a given information type. By establishing an agreed national and international '*baseline*' for CSF protection profile applied to a given information type, with controls based on an assessment of information risk. The CSF protection profile baseline sets the agreed upon minimum accepted cybersecurity controls for an information type. These controls can consist of cybersecurity controls from any cybersecurity standard and can be added to by a nation in line with its own national security requirements, thereby harmonising cybersecurity standards across the U.S, EU and APAC. When an agreed upon baseline is harmonised nationally and international for an information type, harmonised oversight and assurance can be performed by internal audit in the form of a self-assessment or competent regulated third-party assessment, for example AICPA.

Contracting organisations within the government or commercial organisations can either choose to use the self-assessment, negotiate a third-party assessment and/or add additional controls commensurate with the level of risk as determined within a contract. As the controls documented within the protection profiles using the CSF can include any controls framework (e.g. NIST SP 800-53, ISO 27001, Cloud Security Alliance), it establishes a basis for reciprocity ensuring that an adequate assessment can be achieved globally. These assessments provide assurance as to the adequacy of controls across the international landscape which has been a challenge that has not yet been addressed, but we feel can be addressed by this proposal. This approach respects international sovereignty and can help create international buy in for this approach.

Because the process of common criteria is already in place we feel it is logical to apply it to cybersecurity regulation and information types

How can we help

We want to work with you to shape and implement cybersecurity risk management policy within the U.S and between the U.S. and its international partners. Our common objective and goal is the harmonisation of national and international cybersecurity policy, legislation, and regulation as well as satisfying the assurance requirements of the U.S government.

We can leverage our cybersecurity and cybersecurity risk management experience in the design and delivery of cybersecurity risk management regulations, products and services across both 1st and 2nd Lines of Defence across many industry sectors. We provide advisory services to public sector organisations and Federal programs that have included the CMMC. We are skilled cybersecurity, risk management and cyber education

practitioners, that understand the challenges faced with creating, delivering, and providing oversight and assurance of cybersecurity risk management. Having implemented national and international cyber security risk management standards and delivered numerous cyber risk management courses across most Federal agencies.

References

1. Common Criteria: https://en.wikipedia.org/wiki/Common_Criteria
2. National Information Assurance Partnership: <https://www.niap-ccevs.org/>