UNDERSTANDING AND MEETING DISP INFORMATION SECURITY REQUIREMENTS

How to Manage Supply Chain Risk with DISP Enabling Information Security Strategies

archTIS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The supply chain brings a network of interrelated companies, services, and products in combination to transform raw materials and information into goods and expertise used to deliver to a final user or consumer.

Given the scale, breadth, and complexity of bringing so many different things together, the risks that a supply chain presents can be difficult to define and manage. There are so many different interactions and inputs, that an interruption at one point may ripple out to have global impact.

The complexity and the associated risks mean that supply chains present a significant potential impact to sovereign capability and national security. So much so, that the Australian Productivity Commission (PC) released a significant Interim Report in March 2021 on Vulnerable Supply Chains. While this interim report focuses on global supply chains (and Australia's resilience to disruptions in these chains), many of the principles apply equally to any sector of the economy, including the Defence supply chain.

The industries and businesses that supply into this complex chain present both risks and challenges at the same time as they provide important input to capability. Government services, including Defence need to always be operational and maintain a state of readiness to respond to security and safety emergencies.

This white paper will explore supply chain data security risks, and how the Defence Industry Security Program (DISP) aims to help businesses to address the risks associated with providing services, products, or capability to Australian Defence. It will also explore how to meet compliance requirements with DISP ready information security strategies.

WHAT MAKES THE SUPPLY CHAIN VULNERABLE?

The term “Supply Chain” has been in the news a lot recently, whether it has been due to the reduced ability to manufacture and ship components due to a worldwide pandemic or that the “Supply Chain” has been compromised via an IT security non-compliance or insider threats.

With end clients expecting high quality goods and short delivery timelines suppliers are having to make decisions quickly, around whether to insource / outsource / right shore the manufacturing of each and every component that makes up the final product (solution) that they are delivering and how to ensure end to end security over these critical communications - conversation, business documentation, architecture plans and customer details.

Each and every decision that is made to include additional (external) components into a final product, adds extra linkages and complexity into the flow of the supply chain. If we define “Supply Chain” as an agreement that exists between a company and its suppliers to produce and distribute a product to an end user. Depending on the product this Supply Chain could be as simple as Supplier and Retailer relationship, to a more complex flow that include numerous producers, vendors, warehousing, transportation and retailers.

Whatever the makeup or length of the Supply Chain the requirement for efficient and secure communications, collaboration and sharing of business files are essential to ensure that the product is delivered 100% as per the designed specifications - not in a compromised state.

With so many Supply Chain members, possibly spread across the globe, involved in every delivery element of the manufacturing of a single product - industry has had to innovate and utilise software tools (often bespoke) that can enable them to communicate, provide management over just in time production, delivery and ongoing support. It is at this point where the emergence of cyber management needs to be introduced alongside the traditional supply chain components.

The impact of a Supply Chain cybersecurity breach or failure can be devastating to suppliers, consumers and bystanders alike.

The impact caused by an interruption to a real-world supply chain is massive as the Colonial Pipeline in the United States showed when a cyber-attack resulted in the shutdown of this major oil pipeline causing widespread shortages of fuel across the Southeast United States. Beyond the brand and financial repercussions for the Colonial Pipeline, it spurred panic buying (hoarding) within the public, as well as the unknown and undocumented ripples that it caused in the downstream processes within both domestic and international markets.

From this one example of a cyber-attack of a single mission critical Supply Chain, it is evident that a breach impacts not only the supplier of service - but also extends to the greater community at large.

Understanding Risk in the Supply Chain

The vulnerability of these supply chains to interruption (whether intentional or accidental) is a significant focus for governments and organisations, so much so that the Australian Productivity Commission (PC) released an Interim Report in 2021on the vulnerability of these global supply chains.

The report highlighted a number of Key Risks factors in the modern supply chain that increase firm-level risk to include:

- Lack of flexibility (dependency on one firm for a critical input)
- Geographic clustering (if all the firms in an industry are in one location)
- Long supply chains (how many times goods change hands and countries)
- Infrastructure-related shocks, such as cyberattacks or disruptions at a port or along a road.

All of these factors illustrate the need for communication at speed, across multiple locations to complete the end-to-end process.

In the Defence context, there are additional risks associated with the sensitivity and security classifications of information, systems, and capabilities. These sensitivities require participants to redefine their processes to meet these defence requirements.

The Defence industry is global, complex, and massive - with thousands of companies, millions of people, and trillions of dollars in expenditure around the world involved, delivering both products and services that are needed for Defence capability. The Australian Defence industry alone is an AUD $38.6bn annual market in 2021 according to IBISWorld.

This scale and complexity alone are already a major challenge for participants as they seek to manage their risks, with significant security, technology, personnel, and financial considerations to manage.

With all this connectivity comes RISK.

HARDENING THE SUPPLY CHAIN WITH THE DEFENCE INDUSTRY SECURITY PROGRAM (DISP)

To help address and protect against these major supply chain issues the Australian Defence Organisation introduced the Defence Industry Security Program (DISP) for those providing services, products, or capability to the Modern Australian Defence Force, either directly or indirectly.

Managed by the Defence Industry Security Office (DISO), the intent of the program is to both guide and assess the businesses that may form part of a complex supply chain for Defence. DISP guidance and assessment encompasses processes, procedures, information technology (IT) and cyber security, physical security, and personnel security.

DISP forms part of the broad framework of risk management across the complexities and challenges that Defence needs to operate within, to delivering their objectives. It also helps them to apply the experience and expertise that Defence has in operating in complex and security-conscious environments, helping Australian businesses improve their security governance implementations.

Australian Defence Department (ADoD) recently highlighted four major cyber threats to the defence industry in a recent paper - Working Securely with Defence 2020:

- Foreign Government / state sponsored attacks
- Cyber Crime
- Human error and Insider Threats
- Risks in global and local supply chains

Each of these threats bring their own unique risks to the ADoD, for example a breach in the Defence industry supply chain could cause a degradation of services, loss of sensitive information or even the shutdown of vital supplies.

To assist further with the mitigation of risk across its critical supply chain, the ADoD introduced a revamped membership program for the Modern Defence Organisation – DISP 2019 – to assist protect its integrity and capabilities.

DISP acts as a set of mitigation guidelines and measures that assist and benefit Supply Chain members to harden their policies and procedures when supplying goods and services to Defence. At a high-level DISP helps business to:

- Understand, deliver and maintain their security responsibilities;
- Create and implement governance policies and practices to assist in the mitigation of risk;
- Protect the assets and sensitive information that make up the supply chain;
- Security training plus advice and analysis on the latest trends and threats

The Intent of DISP is to reduce and mitigate the forever-evolving security threat to ADoD infrastructure, assets and people and its suppliers. The DISP certification has almost become a standard requirement for those that deal with ADoD, especially when there are multiple contractors involved in the delivery of a product. The DISP membership allows potential business partners to be confident that they are dealing with a like-minded supplier that have all the governance and process rigor required by the ADoD.

THE TOP 4 SECURITY ELEMENTS OF DISP

1. Personnel Security
2. Physical Security
3. Information Security
4. Security Governance

DISP CERTIFICATION REQUIREMENTS AT A GLANCE

DISP Certification is required if suppling one of the following items:

- Handling or working on sensitive/classified information or assets;
- Storing or transporting Defence weapons;
- Providing security services for Defence bases and facilities; and/or
- As a business requirement to their offering.

To participate in the Defence supply chain, businesses can apply for DISP membership, that will assist in the certification of the business that will improve their processes by strengthening these four core pillars:

Personnel Security

- Comply with standards
- Management of clearances
- Reporting

Physical Security

- Determining the security and requirements for business premises

Information Security

- Compliance and standards
- Communication and information sharing risks

Security Governance

- Ensuring that you have staff focused on the security of the business
- Run awareness programs on the latest cyber threats
- Annual Reporting

On the surface gaining certification looks to be a follow the bouncing ball process to accreditation. However, very often this is just the beginning of a complete internal business process and policy refit, plus infrastructure revamp.

Attaining DISP is not a simple off the shelf solution. It requires focused (if not dedicated) personnel, facility hardening, corporate governance enforcements, cyber policies and infrastructure. All elements that add costs to the art of doing business with ADoD.

With the majority of the certifiable elements focused on internal governance (policy / procedure) enforcement and reporting, it is difficult to understand where existing technologies can assist you attain certification and underlay your new established governance directives.

One of the four key pillars where technology can greatly assist is information and cyber security.

Systems used to handle, process or store information that is sensitive to the Australian Government requires a process of validation and risk assessment called accreditation.

MEETING DISP INFORMATION SECURITY REQUIREMENTS

Systems seeking this accreditation are required to meet stringent and comprehensive controls of both a technical and non-technical nature.

The controls, guidance, and verification within the Australian Government Information Security Manual (ISM), the Protective Security Policy Framework (PSPF), as well as the ASD top 4 security elements are expected to be addressed in part by these systems, as well as the premises or facilities in which they reside.

Reducing Complexity and Cost

The complexity of designing, building, and accrediting an environment to satisfy these requirements is a significant challenge, requiring specialists with deep experience, along with careful planning and comprehensive technical expertise. There is a need to maintain the environment in line with the security expectations of the government clients, as well as the risk management expectations that come with handling classified information.

Appropriately securing the physical premises, the information systems, and the personnel needed represents significant cost and complexity to organisations. This results in environments of this nature being prohibitively expensive, both to build and maintain. Expertise in ICT and security is expensive, as is the cost of purchasing and maintaining ICT equipment.

With expensive specialist resources and equipment, the cost of even a basic ICT environment accredited to a PROTECTED level for a small number of users can be extremely costly to build (and even more expensive when considering larger organisations with more complex needs), plus the ongoing costs of sustainment and support.

Some companies have the scale, budget, and personnel to create and manage systems and environments that can be approved to process sensitive information from the government. These environments and systems require ongoing specialist management, to ensure that the security validations are maintained.

Even then, the information is sometimes of limited value, being only relevant and available for a limited context, meaning the dynamic and changing nature of a supply chain becomes even more difficult to address.

The Small and Medium Enterprise (SME) participants of the Defence supply chain are also at a distinct disadvantage here, often operating without the capital or access to specialist technical expertise required to address these security barriers.

Is it really a requirement to maintain your own infrastructure to have an accredited secure ICT information and collaboration platform that is utilised to underpin your process and policies?

The answer may surprise you, but no.

While a company in the Defence supply chain needs to have a set of processes, policies, and business practices in place to ensure they understand their responsibilities and requirements of participating, it is not a requirement that the IT systems for the sensitive information handling be operated by them directly.

The key here is to a have a solution that assists you with meeting certification and internal governance and reporting obligations.

ACCELERATE YOUR DISP MEMBERSHIP WITH KOJENSI

Kojensi is a proven and accredited platform for classified information collaboration and file sharing that enables productivity, while managing the level of compliance and security of information required by DISP.

It provides a simple and secure cloud-based solution for collaboration and storage for files and documents up to and including Australian Government PROTECTED information.

Enforcement of Content Governance

As a fully hosted platform Kojensi allows business to separate sensitive or classified Defence information from their corporate systems, providing an easy-to-use platform to apply process and rigor required to implement the Information & Cyber Security governance required for DISP membership.

Access Control and Secure Workspace

Kojensi enables information owners to set and enforce strict security controls over information, using the zero trust methodology to enforce Attribute Based Access Control (ABAC). It provides file access based on a user's organisation, nationality, clearance, and compartmentalisation of information. Allowing users to share information securely between multiple organisations, at multiple classifications, and across different jurisdictions – while meeting compliance and security requirements.

Kojensi ensures that access to a file is ONLY granted once a user meets all the specified release requirements, defined by the ABAC policy which looks at user, file, and environmental attributes before granting access. These files can also be restricted from editing and download - reducing the risk of insider threats – in real-time.

Kojensi's ABAC policies offer many benefits and afford granular data security to not only ensure compliance, but to also ensure operational security by delivering a seamless zero trust solution to securely deliver and share information to Supply Chain partners.

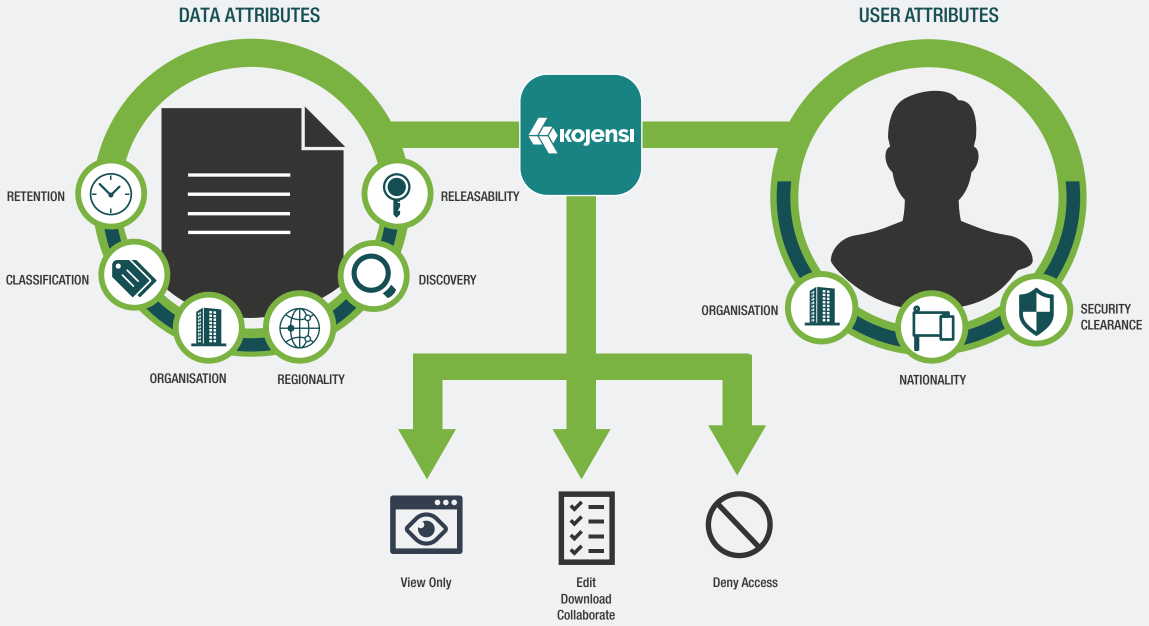
Audit and Accountability

Every action performed in the Kojensi portal is logged and timestamped for auditing, transparency and remediation if required. You can also integrate user activity and logs with SIEM tools for downstream analysis.

System and Information Integrity

Kojensi compartmentalises data and users to prevent over privilege abuse ensuring both product and local administrators cannot override the workplace security.

KOJENSI DELIVERS REAL TIME, ATTRIBUTE-BASED ACCESS CONTROL



CONCLUSION

Kojensi allows business to separate sensitive or classified Defence information from their corporate systems, helping to quickly meet criteria for the Information Security required for DISP membership.

Talk to us about how we can help accelerate your DISP membership today.

ABOUT ARCHTIS LIMITED

archTIS Limited (ASX:AR9) is a provider of innovative software solutions for the secure collaboration of sensitive information. The company's award-winning data-centric information security solutions protect the world's most sensitive content in government, defence, supply chain, enterprises and regulated industries through attribute based access and control (ABAC) policies. archTIS products include Kojensi, a multi-government certified platform for the secure access, sharing and collaboration of sensitive and classified information; and NC Protect for enhanced information protection for file access and sharing, messaging and emailing of sensitive and classified content across Microsoft 365 apps, Dropbox, Nutanix Files and Windows file shares. For more information visit archtis.com. Follow us on twitter @arch_tis

archTIS

archTIS.com | info@archtis.com

Australia | United States | United Kingdom