ADIESA
Australian Defence Information and Electronic Systems Association

Mailing address: PO Box 3869, Manuka, Australian Capital Territory, 2603 - ABN: 53 620 349 109

Cross-domain working group report

Contents

Summary of Key Themes

Industry recommends that Defence consider the following themes brought out in this paper:

- Promote the CDS community within Australia through active engagement in online forums, conference attendances and presentations.
- Release roadmaps and forecasts around CDS initiatives, to allow Australian industry to prepare for emerging opportunities and pursuits. In order to solicit the best capability for Australia, Defence would benefit from providing industry with a longer term view on future Cross Domain Solution needs which will provide guidance to industry about the right level and direction of investment into Australian CDS capability (including international reach-back).
- Collaborate across Defence programs and organisations in sharing and reusing CDS solutions. This includes reusing the solution itself, the design and security documentation, or the implementation and sustainment arrangements.
- Promote a multi-vendor contribution to the overall CDS solution. Industry can develop pockets of excellence and reach a diversified and sustainable state.
- Assist/sponsor Australian Industry to develop and apply new innovative solutions to solve Australian cross domain challenges, such as through the use of the DSTO/Capability Technology Demonstrator program. This is expected to provide an enhanced set of offerings to qualify for listing on Defence's Evaluated Product list (EPL).
- For Defence to review the capacity of its existing accreditation bodies to ensure that Defence has the right size teams for certification and accreditation activities, with one benefit being the more predictable project scheduling through these activities.

ADIESA welcomes further collaboration with Defence and will gladly facilitate future discussions between the ADIESA membership and any organisations within Defence. If an organisation within Defence would like to discuss any of the issues identified in this paper further with the ADIESA members, we would be pleased to oblige.

Introduction

Purpose

1. The purpose of this report is to provide a consolidated Defence Industry (ADIESA) view on Defence's future Cross Domain Transfer capability. This report was requested at the Defence/ADIESA ISREW Focus Group Meeting of 4 March 2015 by the Defence sponsor.

2. The views expressed in this report reflect the experiences of the authors and ADIESA membership, but do not necessarily constitute the common and agreed position from all ADIESA member companies. Within this report the term Industry is intended to reflect ADIESA member's perception of the broader Industry perspective.

Scope

3. A cross domain solution (CDS) is defined in the Information Security Manual (ISM)[1] as "An information security system capable of implementing comprehensive data flow security policies with a high level of trust between two or more differing security domains".

4. In consultation with the Defence sponsor, the scope of this paper is limited to Cross Domain (Transfer) and excludes CDS (Access) and CDS (Multilevel). A transfer CDS facilitates the transfer of information, in one (uni-directional) or multiple (bi-directional) directions between different security domains[2].

5. ADIESA's understanding of cross domain also includes Australian Secret to US Secret where the classification is the same but the information crosses national boundaries; because they are governed by different security policies. The rules for when Cross Domain is required are (i) where one domain is Confidential or above, and (ii) If the same level but governed by different security policy. Fixed and deployed networks at the same classification level such as Defence Secret Network (DSN) to Deployable DSN (DDSN) are both covered by the ISM and therefore do not require a CDS, although a gateway is common practice.

Intended Audience

6. The intended audience for this paper includes:

- Defence Force and Capability designers to acquaint them with broader capability definition and development options.
- Defence policy makers such as ASD and CIOG (who have a role in setting acquisition and maintenance policies applicable to CDS) to acquaint them with acquisition and support options that are outside Defence's current visibility.
- Defence operational users of a CDS to acquaint them with a consolidated industry viewpoint
- Other government users (such as DFAT) to acquaint them with the broader industry issues
- ADIESA members as a foundation for building a sustainable workforce in CDS

Industry Issues (Why is this paper important?)

7. Australian Industry is an important contributor to the security of the Australian Government and its information systems. In the case of Cross Domain Security, Australian industry has a wealth of expertise and experience, capabilities and services, which can assist the Commonwealth in delivering secure and robust cross domain data transfer capability. Coupled with an ability to leverage the resources and experience of their parent companies, Australian Industry has the ability to be a key partner in assisting the Commonwealth to achieve the secure sharing of information between security domains and enclaves.

8. Guidance from the Commonwealth will assist industry in gaining a better understanding of the Commonwealth's cross domain requirements and will allow industry to provide better and more timely responses back to Defence.

9. An understanding of the ASD requirements for the secure deployment of cross domain solutions will also allow industry to architect secure solutions that meet ASD's mandated requirements and will

[1] ISM page 302
[2] ISM page 264

subsequently reduce the Certification and Accreditation risk to the relevant project. Cross domain capability will be provided as part of the solution architecture, not as a bolted-on afterthought.

Slow progress of effective CDS in Defence

10. At a Federal level, the Australian Government's National Security information Environment Roadmap and 2020 Vision states the increasing need to explore opportunities to seamlessly move information from one classification domain to another ('cross domain sharing'); enhancing the ability of the national security community to collaborate and share information at the highly classified level. Technology, in the form of Cross Domain Solutions, enables and automates these information sharing business decisions, while ensuring the privacy and security of that information. Nearly all programs on the 2012 Defence Capability Plan that have an element of information and communications technology, have a Cross Domain requirement, demanding data confidentiality, integrity and availability.

Policy Issues

11. The only publicly available policy is the ISM. Other material guidance is classified, with no recognised path for general industry access.

Accreditation

12. In the ASD Cyber Security Operations Centre publication Network segmentation and segregation (Sep 2012); the chapter "What is Network Segmentation and Segregation", details some of the common technologies and methods to achieve this, including "Implementing DSD-evaluated cross-domain solutions (CDS) where necessary". Unfortunately, the current Evaluated Products List[3] does not include any evaluated cross domain products.

13. The Australasian Information Security Evaluation Program (AISEP)[4] tests ICT security products for possible inclusion on the Evaluated Products List (EPL). The Australian Signals Directorate's certification office, the Australasian Certification Authority (ACA), oversees AISEP product testing by licensed commercial evaluation facilities. Australasian Information Security Evaluation Facilities (AISEF) are licensed to perform AISEP evaluations and have been accredited by the National Association of Testing Authorities, Australia (NATA).

14. ASD has the sole responsibility, in Australia, for evaluation and accreditation of cross domain data transfer solutions. For Defence systems up to and including SECRET, the Defence Chief Information Officer's Group may accredit systems, under the guidance of ASD. As part of its accreditation process, ASD does engage with the US United Cross Domain Services Management Office, for the exchange of technical data and advice.

15. ASD are responsible for CDS advice and guidance, then vulnerability assessment leading to a risk report. The risk report is attached to ICT Security Branch's (ICTSB) ISM certification report with recommendation (by ICTSB) and sent to Head ICT Operations (HICTO) (accreditation authority) to make the accreditation decision.

16. Additionally, Cross Domain solutions are evaluated and accredited to operate in a specific environment, transferring specific file types and with specific data channels. Hence, each unique implementation of a cross domain solution requires the system to proceed through a full accreditation and certification process, even if the cross domain product and architecture remains unchanged. This poses a

[3] http://www.asd.gov.au/infosec/epl/index.php
[4] Cited from http://www.asd.gov.au/infosec/aisep/index.htm

significant impost on limited ASD resources as well as a significant risk to the project timeline, given that certification and accreditation processes can take between 12-18 months, leaving a technical solution open to being leap frogged by the technology cycle. By the time a specific solution is put into production it can be already out of date, giving rise to issues including a reduced support horizon and potential new vulnerabilities that have to be managed. Due to the inherent risk profile of a CDS, it is important that it is based on current, patched technology that is as up to date as possible.

17. ASD's OnSecure website could be a useful tool for the government CDS community to connect with the industry CDS community, and share ideas and technological developments. Unfortunately there is no active discussion forum regarding CDS and there is only limited material for the community to access. For the community to participate on OnSecure they require both a justification for access (which can be difficult for industry); and there needs to be up-to-date, relevant material to attract them. Industry recommends that Defence uses OnSecure to encourage industry to participate and build the CDS community through the website. This can be done through two activities:

a. First, for Defence to maximise participation on OnSecure by opening up access to contractors who are only occasionally involved in government.

b. Secondly, for Defence personnel to be encouraged to post content, draft policies/whitepapers etc, to attract the community, and allow members to learn, contribute and engage.

What is aggravating industry?

18. Acknowledging that ASD is the centre of excellence in Australia for cross domain issues, there is little in the way of publically available, documented guidance from ASD. Historically projects have been subject to disjointed accreditation of individual elements, with the result that there is no clear understanding of the planning parameters for a cross domain project.

19. An accurate, fully costed quotation of a cross domain solution is difficult to provide given the uncertainty around the certification and accreditation process, the subsequent timeline and therefore the total cost. Similarly, an accurate project plan and project schedule for a cross domain solution is also problematic, given the same uncertainties around the process and its timeline.

20. Defence projects typically manage cross domain solution risk with a time and materials contract for the CDS component of an acquisition. As the demand for CDS increases, with increased levels of interoperability and integration, it will become increasingly difficult for industry to make firm fixed price estimates for system-of-systems programs.

Industry Support to Policy Issues

21. Industry won't be there to support Defence unless it is a sustainable industry.

A UCDSMO Focus Limits Capability Offering by Australian Industry

22. The US-based Unified Cross Domain Services Management Office (UCDSMO) maintains a validated list of approved baseline products deployed within the US Department of Defence (DoD) and the Intelligence Community (IC). In recent years Defence has had significant focus on application of UCDSMO approved products to the Australian context. While UCDSMO is an invaluable organisation to leverage, industry has identified some limitations in being tightly bound to UCDSMO practices.

23. Industry acknowledges that use of UCDSMO approved products provides a strong maturity baseline for Australia as well as coalition interoperability benefits, however strict focus to this list of products creates

limitations for Australian capability (both for Defence and Industry). Moreover, as UCDSMO listed products have been accredited to fulfil a specific US need, Defence would be better placed to reach out to Australian Industry to provide their best solutions without being limited to those with UCDSMO listing.

24. Industry understands that a solution can't be on the UCDSMO list unless it is active in a US program. That is, a US based program identifies the need at the program level, this leads to a product being accredited, then purchased and installed, and then finally being put on the UCDSMO list.

25. Australian Industry highlights that the UCDSMO list only contains products that have been already been certified and accredited for use, and therefore limits the global industry capability available to Defence. Specifically this presents two challenges:

a. For Australian Industry to gain support for developing new products indigenously, and

b. For Australian Industry to bring in new global product, technology and methodology offerings from Industry's international market base.

26. Australian Industry would be better positioned to look beyond the UCDSMO baseline to create or apply those Cross Domain Solutions tailored to Australian needs, if Defence was more receptive to non-UCDSMO solutions and technologies.

27. In addition, in order to be able to put the best capability forward for Australia, Defence and Industry would benefit from a longer term view on the future enterprise CDS roadmap. Defence has done this well based on recent enterprise wide initiatives, and any further guidance will help industry grow local capability either through indigenous development or leverage of international expertise.

Combating the ITAR Challenge

28. Defence and Industry recognise that managing technical data and services constrained by the US International Traffic in Arms Regulations (ITAR) is challenging. ITAR comes with an overhead in effort for access, handling and control. Technical Assistance Agreements (TAAs) need to be established once an opportunity area is qualified and typically require significant lead times to establish.

29. Furthermore, Australian Industry experience challenges in developing the appropriate local knowledge on the depth of global capability available within their own global companies due to ITAR constraints in absence of an established TAA. This has four impacts on Australian business which the affects Defence:

1. Australian companies are less educated on CDS technologies
2. Support and implementation skills are more frequently sourced from the US at typically higher cost
3. Australian companies have less visibility of existing and emerging US developed CDS technologies and practices, in order to provide innovative proposals to Defence, and
4. This reduces the Australian Industry capability and capacity to support implemented solutions.

30. To combat this challenge, with early guidance from Defence, Industry can start early to establish the appropriate TAAs to support future Australian needs. In addition, this will provide argument for Australian Industry to invest and build the appropriate local and cleared staff to support Defence, which in-turn is expected to deliver tailored solutions with improved responsiveness at a lower cost.

31. Because of the inherent sensitivities of CDS, it is difficult for a community to grow among government, industry and academia. A CDS community in Australia would allow the constituents to build relationships, learn about emerging technologies and methodologies, discover new frameworks and share experiences.

Forums such as OnSecure are valuable, but only when the community is active, and the content up to date. OnSecure also has a limited access policy and can be difficult for industry and academia to access without an ongoing, specific requirement. Defence can invigorate these communities by uploading announcements and other suitable material.

Industry Support to Accreditation Issues

32. Industry perceives a lack of visibility over the accreditation process. Industry understands for the ASD Vulnerability Assessment process that the vulnerability test (strategy/plan/cases) and test results are by default all highly classified. It is difficult as a planning exercise to interlock a project plan with anything more detailed than an estimated start and end date for vulnerability assessment, with no further visibility. Particularly for downstream activities that are dependent on the results of the vulnerability assessment, there is the opportunity for Defence to work with Industry at the project planning level to improve the timely allocation of resources for the benefit of the project, and Defence and Industry more broadly.

33. The lack of visibility raises questions over the efficiency of the accreditation process. Industry suggests that there may be a streamlined approach possible towards accreditation so that one minor change does not invalidate the previous work done. Patching and upgrading normally apply, but addition of new functionality is a very much more substantial issue in a CDS, which introduces risks to the current accreditation. Industry's understanding of current Defence priorities is to achieve economy of scale via centralisation, and this ensures adequate funding for scheduled yearly technology refresh (minor and major upgrades) to keep up-to-date and therefore maintain the appropriate level of security.

34. The sector of industry that helps with capability definition assesses that the biggest issue is trust within Defence of the accreditation process, as evidenced by the various Defence projects which are reluctant to trust other parts of Defence in this area and also the broader issue of how to get Defence to trust Industry.

35. Industry accreditation issues include a lack of enough knowledgeable personnel within Defence for this function, which can represent a single point of failure when key people move as evidenced by the long lead times for the accreditation process.

Cross Domain Reference Model

36. A Cross Domain Reference Model (CDRM) would allow agencies to standardise across Transfer CDS instances. It will provide a high level framework that would articulate functions and some indication of their interfaces and interactions with each other and with functions located outside of the scope of the reference model.

37. With implementing solutions in accordance with the CDRM, agencies will be able to get consistency across the solution gaining advantages in components such as:

a. Ability to get a standardised platform to make it easier to evaluate any responses to tenders by industry.

b. Getting a known baseline which should reduce cost and time of a CDS solution.

c. Make is easier to get accreditation as by staying inside the framework, accreditation agencies will have a known baseline.

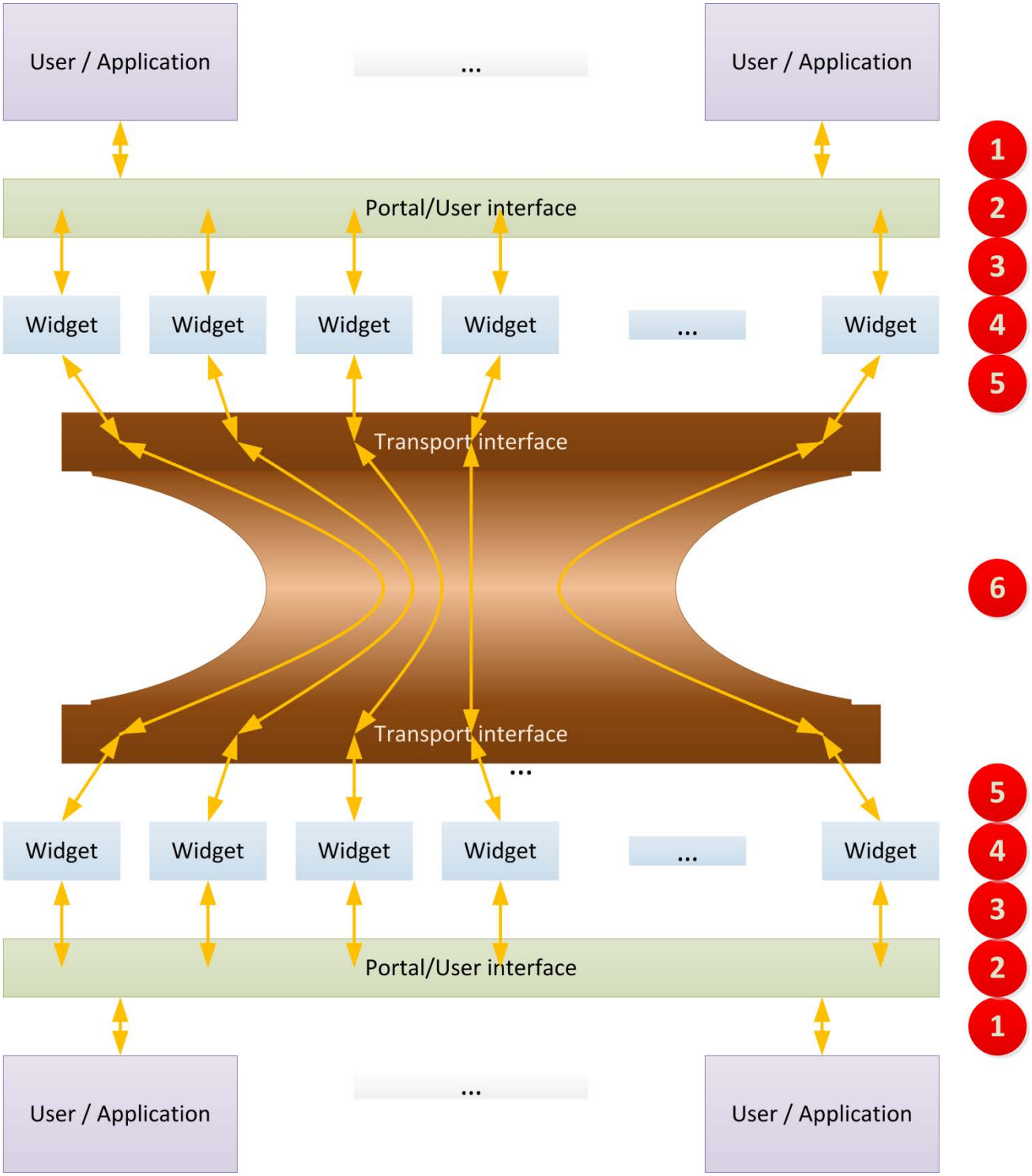

Figure 1 Cross Domain Reference Model (CDRM)

38. With reference to Figure 1, the "widgets" are the elements of software or services that check each file to see if it safe to send. These are technology/format specific.

a. Strategy 1: Positive clearance: [Find reasons to send it through] Look for the defined structures within the message that are security markers. E.g. XML elements that hold the paragraph classifications.

b. Strategy 2: Negative clearance: [Find reasons to not send it through] Dirty word checking

c. Strategy 3: Malware checking: [Look for bad things].

39. Each strategy can be used in combination. A failure for any strategy will mean the file will be sent to the manual process for further checking/evaluation.

a. The portal and transport interfaces are technology/format agnostic.

b. The portal needs to recognise formats/technologies in order to send to the right widget.

c. The portal handles authorisation of users.

40. The transport interface only needs to know if the file is OK to transmit and which widget at the other end to send it to.

a. The users only see the portal and have no visibility or interaction with the layers underneath.

b. This modular framework means that accreditation is done in smaller chunks. And a change in one section does not mean that the entire solution needs to be accredited. The following are the accreditation points.

i. The way the user interacts with the portal.

ii. The portal. Importantly, can the portal find the right widget?

iii. The link between the portal and a widget. If a new widget is put in place, only (3), (4) and (5) need to be assessed.

iv. The widget – can it correctly assess the files? The widget will be unaware of "who" and "why".

v. The link between the widget and the transport layer.

vi. The transport layer itself.

c. Logging and governance of each layer will be a consideration in the accreditation process.

41. An important consideration is that any vendor can contribute to the overall solution. Industry can develop pockets of excellence and reach a diversified and sustainable state.

42. Figure 2 provides a sample functional view of the Cross Domain Reference Model. This can be broken down further and have other functions added. However, any framework must be product agnostic, including where a particular type of CDS provides a specific function. Any product specific functions should not be included in the CDS Framework. The reference model can have multiple views. The functional view is important – but a services view, an operational view etc are also relevant to ensuring a shared understanding. The diagram above provides a capability system perspective – how does it all fit together in the broader picture. The diagram below is more strictly functional. However – both diagrams are needed to ensure that Defence gets the capability it needs.

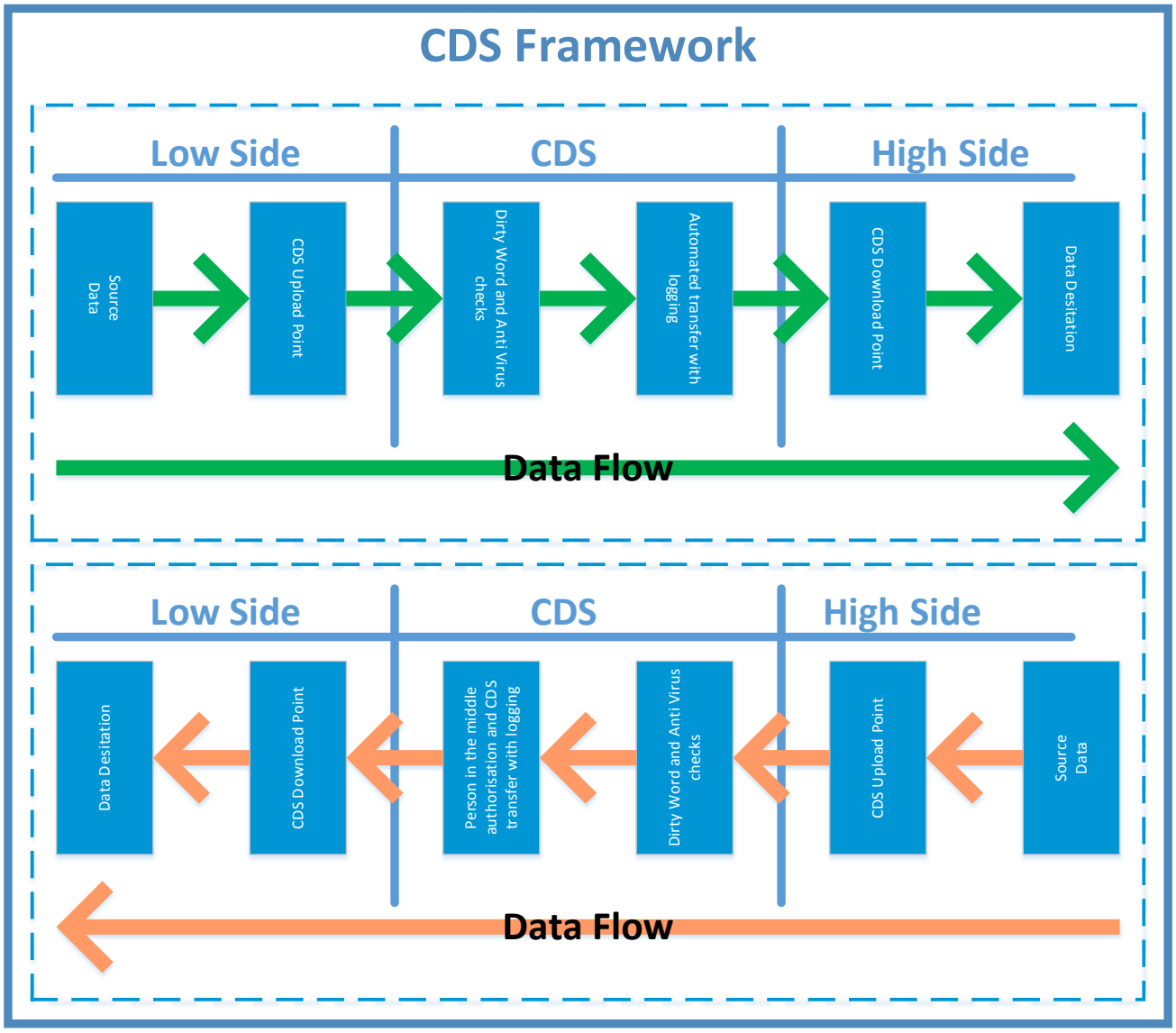

Figure 2 - Sample CDRM Functional View

Other FIC - Industry Options

43. Defence uses the Fundamental Inputs to Capability method to describe a capability, as described in the Defence Capability Development Handbook 2014. While the capability development processes are inherently flexible, Defence has traditionally used Industry for the delivery of Major Systems, with some support activity included. Defence has not, traditionally, used Industry for a coherent approach to the full range of FIC – any other approaches are usually considered in the vein of temporary resourcing measures[5].

44. Importantly, Defence can partner with Industry (e.g. through industry associations such as ADIESA) to ensure a holistic approach to capability realisation.

[5] This is a generalisation, and some localised examples can be found.

45. The following table illustrates the capability and capacity of Industry to contribute to the cross-domain capability.

Fundamental Input	Industry contribution?	Comments
Command and Management	No	Defence are unlikely to look towards industry for policies, procedures or doctrine. However, Industry may be able to provide information about best practices for the secure transfer of particular data types. ADIESA Members see this kind of support as more of an ad hoc consultancy rather than a formal input to the cross-domain capability.
Personnel	Yes	Industry can provide a stream of skilled personnel to contribute to the capability. Personnel with skills in the secure transfer of particular information types may be developed through engagements outside of Defence and perhaps through international engagements. These personnel could support he ongoing management of the relevant business rules within the context of their specialisation. Personnel with skills in the maintenance of secure information systems can be provided to help support the Major Systems that form part of the capability. This support will be similar to existing ongoing ICT support contracts throughout Defence. The formal recognition of skills will help build a future stable workforce, with the corresponding reduced risks to Defence.
Organisation	No	A specialised Industry sector around the secure transfer of information does not exist. Should such a specialised sector appear, then Defence would be able to formalise the Industry interaction by recognising the interaction within the architecture of the organisation. Such recognition would enable Defence to focus on core skills and business, confident that agreement has been reached with Industry to achieve their role. In turn, this will also allow Industry to have confidence in a growth path and a future stable workforce. The secondment of any particular industry member to form part of the organisation does not seem appropriate. ADIESA recommends that the role of Industry in the provision of the capability be formally recognised in the organisational structure.
Materiel/Major Systems	Yes	The provision of ICT hardware and software to achieve secure transfer follows the path trodden by many Defence projects. Services infrastructure is included as part of this discussion on Major Systems.
Supplies	No	The provision of supplies is not a significant input for ICT systems (with the exception of electricity providers).
Support	Yes	Industry is well placed to provide support to the cross-domain capability. Industry already has a track record for providing maintenance to many systems throughout Defence (and the rest of Government). Industry can provide engineering support through the design of new (or enhanced) cross-domain elements. Given the wide variety of information to be passed, this is more likely to take an ongoing cross-industry strategy than a periodic single vendor approach. The level of support will depend on the architecture chosen by Defence. A federated architecture can allow for economies of scale for global support while still allowing for individual support packages for key elements. This allows for an overall support strategy without necessarily exposing individual industry member's intellectual property.

Collective Training	No	Industry is not currently considered during Defence's collective training exercises. ADIESA recommends that collective training exercises include representatives from the industry sector (e.g. through industry associations such as ADIESA) so that Industry support, or any surge capacity within Industry, can also be assessed.
Facilities and Training Areas	Yes	Industry members within the Canberra region have secure facilities that could be used to transfer information between domains (e.g. Industry rooms for Test & Evaluation). However, ADIESA believes that this scenario will be unlikely as the information will have to be transferred to these facilities in the first place. This does not preclude the use of these facilities as a redundancy measure. More importantly, these facilities can be used for training and testing of procedures and information scenarios, separating the training environment from the technical-operational environment. In this training environment, Industry members as well as Defence can explore the business aspects of cross-domain transfer.
(Information) NOT A FIC	Yes	Information is not a recognised fundamental input to capability. Industry members can contribute to the cross-domain capability by providing information about the information types, in particular efficient means to check for security-related information. This information may include internal data structures, key security markers, procedures, known false positives, and known false-negatives. ADIESA recommends that Defence includes Industry (possibly through a neutral industry association such as ADIESA) throughout the life of the capability to identify enhancements and evolution in information transfers.

Recommendations

46. Industry recommends that Defence consider the following:

- Promote the CDS community within Australia through active engagement in online forums, conference attendances and presentations.
- Release roadmaps and forecasts around CDS initiatives, to allow Australian industry to prepare for emerging opportunities and pursuits. In order to solicit the best capability for Australia, Defence would benefit from providing industry with a longer term view on future Cross Domain Solution needs which will provide guidance to industry about the right level and direction of investment into Australian CDS capability (including international reach-back).
- Collaborate across Defence programs and organisations in sharing and reusing CDS solutions. This includes reusing the solution itself, the design and security documentation, or the implementation and sustainment arrangements.
- Promote a multi-vendor contribution to the overall CDS solution. Industry can develop pockets of excellence and reach a diversified and sustainable state.
- Assist/sponsor Australian Industry to develop and apply new innovative solutions to solve Australian cross domain challenges, such as through the use of the DSTO/Capability Technology Demonstrator program. This is expected to provide an enhanced set of offerings to qualify for listing on Defence's Evaluated Product list (EPL).

- For Defence to review the capacity of its existing accreditation bodies to ensure that Defence has the right size teams for certification and accreditation activities, with one benefit being the more predictable project scheduling through these activities.

Authors (organisation and contributors)

Organisation (alphabetical)	Contributor
BAE System Australia Limited	Nigel Basheer
Dexata Corporation	Mike McMahon
DyerNeed Pty Ltd	Alan Dyer
Hewlett-Packard Australia Pty Ltd	Mariette Lees
Hewlett-Packard Australia Pty Ltd	Peter Breckenridge
Hewlett-Packard Australia Pty Ltd	Tom Harrison
IBM Australia Limited	Doug Stapleton
IBM Australia Limited	Steve Ryan
IBM Australia Limited	Simon Torr
Lockheed Martin Australia Limited	Jonathan Thow
Raytheon Australia	Michael Woods

References

References
2015 Information Security Manual[6]
Defence Capability Development Handbook 2014[7]
UCDSMO website[8]
Evaluated Product List[9]

[6] http://www.asd.gov.au/publications/Information_Security_Manual_2015_Controls.pdf
[7] www.defence.gov.au/publications/docs/defence%20capability%20development%20handbook%20(dcdh)%202014%20-%20internet%20copy.pdf
[8] https://intelshare.intelink.sgov.gov/sites/ucdsmo
[9] http://www.asd.gov.au/infosec/epl/index.php

Glossary

Term	Definition
ACA	Australasian Certification Authority
ADIESA	Australian Defence Information and Electronic Systems Association
AISEF	Australasian Information Security Evaluation Facilities
AISEP	Australasian Information Security Evaluation Program
ASD	Australian Signals Directorate
CDRM	Cross Domain Reference Model
CDS	Cross Domain Solutions
CIOG	Chief Information Officers Group
DDSN	Deployed Defence Secret Network
DFAT	Department Foreign Affairs & Trade
DSN	Defence Secret Network
EPL	Evaluated Products List
FIC	Fundamental Inputs to Capability
HICTO	Head ICT Operations
ICT	Information & Communications Technology
ICTSB	ICT Security Branch
ISM	Information Security Manual
ITAR	International Trade in Arms Regulation
NATA	National Association of Testing Authorities, Australia
SOA	Service Oriented Architecture
TAA	Technical Assistance Agreement
UCDSMO	Unified Cross Domain Services Management Office