Information Security

Critical Information Infrastructure

Frequently Asked Questions

1. What is Critical Information Infrastructure (CII)?

The definition of CII is explained more fully in the CII *Scope and Definitions* document, but a brief summary is:

CII is the ICT components of critical infrastructure, where critical infrastructure is defined as

> those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security[1].

The subset of CII which is owned, operated, or managed by inner budget (IB) agencies is referred to as IB CII (see also the answer to FAQ 8 below). IB CII is defined as those IB ICT assets upon which Critical Services are delivered to the community.

Critical Services

Critical Services are either Essential or Important government services. The loss of confidentiality, integrity or availability of these services would result in serious damage to the physical, social or economic wellbeing of the State. The context for these services is the prevention, or management of, a disaster or crisis.

Essential Services

Essential Services are those government services which, if compromised, would endanger or seriously prejudice the life, personal safety, or health of the whole or a section of the community. Essential Services are those directly related to combating identified threats, the physical survival of the community, and the continuity of executive government (which needs to make decisions to address the disaster or crisis). The primary emphasis is on protecting the lives of citizens.

Important Services

Important Services are those services that are directly related to the physical, economic, legal and psycho-social safety and security of the community, business and government i.e. while Essential Services save the

[1] Australian Government, *Critical Infrastructure Resilience Strategy*

lives of citizens, Important Services save the property, organisations and environments where people live and work i.e. they protect the quality of life of citizens.

To reiterate, the ICT infrastructure used to support Essential or Important services represent CII.

2. How does CII relate to other initiatives?

The Victorian CII initiative is part of a national CII initiative i.e. other State and Territories, and the Commonwealth, have complementary CII initiatives.

3. We already classify our information assets so why do we need to rate them based on CII?

Classification and CII are two different things, although they both use a Threat Consequence table for the assessment:

- Classification is targeted at all of the information assets in an agency i.e. it has a broad agency-wide context.
- CII is targeted at just the information assets associated with Essential and Important services i.e. it has a context of the prevention, or management, of a disaster or crisis, and particularly the protection of citizens lives, and their quality of life, in the face of such a disaster or crisis.

For example, agencies which do not provide front-line services to citizens may not have any CII, but may still have PROTECTED classified information e.g. cabinet documents.

4. Why is the Victorian Government doing this?

Agencies have limited resources, which need to be allocated to the most significant information assets on the basis of risk. The CII process begins the process of identifying and protecting the most significant information assets.

Victoria also needs to play its part in the national CII initiative, and there are significant benefits to be gained from managing the risks to CII (see answer to FAQ 4 below.)

5. What are the benefits of the CII initiative?

Formalising the protection of CII means that the risk of compromise of IB CII is minimised.

CII underpins government services that protect the lives and property of members of the public, and supports their social and economic well being. Any compromise of IB CII can have a direct adverse impact on citizens, and lower their trust and confidence in government information systems and services.

6. What costs, effort and resources are needed for CII?

The costs, effort and resources required will depend on the type of agency, and the preparedness of the agency:

Type of agency

Some agencies (e.g. DTF and DPC) provide services to government rather than directly to citizens. These agencies can be expected to have little or no CII, and the CII cost and effort will be minimal.

Other agencies provide front-line services to citizens (e.g. Victoria Police) and can expect that many of its services will be Essential or Important, and that it will have a high level of CII. For these agencies, the CII cost and effort will be much higher.

Preparedness of agency

Those agencies which have already defined their services, and have mapped their ICT assets to these services, will only have to determine whether a service is Essential or Important, and then nominate the related ICT assets as CII. They will then need to complete a *CII Health Check* for each CII asset. Overall, the CII process will be relatively straight-forward.

For those agencies which have not previously defined their services, and have not mapped their ICT assets to these services, it is likely that significant effort will be required to accomplish this. However, existing documentation (e.g. Business Continuity Management) may provide much of the information required. These agencies will need to define their services, determine whether any services are Essential or Important, and then nominate the related ICT assets as CII. They will also need to complete a *CII Health Check* for each CII asset. Overall, the CII effort will be relatively high.

7. Where is the definition of CII from?

The definitions used within the Victorian CII initiative are adopted or adapted from the comparable definitions used by the Commonwealth and/or other States.

8. What is the IB CII Framework?

The IB CII framework is the formal statement of CII requirements which agencies are required to comply with, and the related tools and templates used in achieving compliance.

9. Why IB CII and not WoVG CII?

Information critical to Victoria may – and often does - reside outside Victoria. WoVG CII includes ICT assets handling critical Victorian information wherever physically located, in any jurisdiction, as well as the private sector. Some WoVG CII may be owned by other governments or agencies.

IB CII is that subset of WoVG CII which is owned, operated, or managed by the inner budget agencies i.e. it is internal to the Victorian Government.

10. What functions/services are in the scope of CII?

See the definitions of Essential and Important services under the answer to FAQ 1 (above).

11. What criteria determine whether assets are CII?

See the answer to FAQ 1 (above).

12. What if my agency has CII assets?

IB agencies must

- record their CII in a *CII Register* using a provided template,
- assess the health of each CII asset, using a *CII Health Check* provided template, and
- take appropriate actions to mitigate the risks to the availability, integrity and confidentiality of their CII assets, and report the status of these risk mitigations annually.

13. What is the difference between the agency CII list and the IB CII list?

The only difference between the two lists is scope. The agency list contains agency CII assets. The IB CII list contains all the CII from the inner budget agencies.

14. What if my agency doesn't have any CII?

If you don't have any CII, you have no responsibilities under the CII initiative.

15. What is the CII Health Check?

The *CII Health Check* is a self-assessment of the information security currently in place to protect each CII asset within your agency. It is intended to assist you in determining where there are gaps in information security governance, risk management, information security classification, protection of personal information, management of outsourced ICT services, business continuity planning, and other CII asset risk mitigations.

16. What should I do with the CII Health Check results?

You should put in place plans to close the gaps identified in the *CII Health Check*, based on the priorities you associate with each gap. (Where your agency accepts the risk associated with a particular gap, no action may be required.)

17. What compliance reporting is required for CII Health Checks?

Mandatory annual *CII Health Check* reports must be completed by the end of December each calendar year. The first *CII Health Check* reports are required by the end of December 2012.

The *CII Health Check* must be submitted to the agency Risk and/or Audit committee, and the agency Executive. A copy of the report and related minutes of the Risk and/or Audit committee must be provided.

The annual *CII Health Check* will ensure executive visibility and oversight of the information security risks to critical services and supporting ICT assets.

18. What is the compliance schedule for CII asset SRMPs, SSPs & SOPs?

Systems Risk Management Plans (SRMPs), Systems Security Plans (SSPs) and Standard Operating Procedures (SOPs), are requirements mandated by the Australian Government Information Security Manual (ISM). They must be developed for all CII assets by 30 June 2014.

The implementation of these SRMPs, SSPs and SOPs may carry forward beyond 30 June 2014. Agencies should list the most important Urgent, Tactical, and Strategic risk mitigations that need to be implemented, submit them to their CISO for approval, and report progress against these risk mitigations in annual CII reporting.