Australian Government

Attorney-General's Department

National Security
Resilience Policy Division

Critical Infrastructure Protection

Modelling and Analysis Program

Tasking and Dissemination Protocols

May 2009

CIPMA Tasking and Dissemination Protocols

Table of Contents

Attachments

Introduction

The Critical Infrastructure Protection Modelling and Analysis (CIPMA) Program is a key initiative in the Australian Government's efforts to enhance the protection of Australia's critical infrastructure.

CIPMA is a computer-based capability which uses a vast array of data and information from a range of sources (including the owners and operators of critical infrastructure) to model and simulate the behaviour and dependency relationships of critical infrastructure systems.

The Attorney-General's Department (AGD) is managing the CIPMA Program and is working closely with Geoscience Australia (GA) to develop the capability. These two organisations comprise the CIPMA Program.

Attachment A provides an indicative schedule of the tasking process that will operate during 2009.

These protocols have been developed to ensure the orderly and transparent tasking of CIPMA, the appropriate and secure dissemination of results, and that the integrity and confidentiality of the data and models is safeguarded at all times. Background information on the development of the protocols may be found on the Trusted Information Sharing Network – www.tisn.gov.au.

Attachment B contains glossaries on the acronyms and abbreviations used in these protocols, details on the security classification levels and an explanation of terms marked (*) in the protocols.

Any questions on the CIPMA Tasking and Dissemination Protocols should be directed via email to:

CIPMA Project Officer
Modelling and Analysis
Critical Infrastructure Protection Branch
Attorney-General's Department
Email: cipprojects@ag.gov.au
Telephone: 02 6141 2951

2. The Tasking Protocol

Stakeholder tasking of the capability will be aligned to those tasking requests for which data and information is currently held or can be quickly and easily obtained. At this stage of CIPMA's development, data collection and modelling is focussed on five priority sectors: Banking and Finance, Communications, Energy, Water and Transport. Other sectors will be added as soon as possible.

As the scope of CIPMA broadens in coverage to include additional data, information, and industry sectors, the ability to task the capability will also broaden over time.

All tasking requests and related scenarios need to be realistic and focus on addressing the high priority issues of risk management in critical infrastructure protection, counter-terrorism, and emergency management. Tasking requests received from business and government stakeholders will be prioritised against pre-determined and transparent criteria.

These criteria include identifying the relative merits of each request and the data and the resources that will be required to run each scenario. The criteria also seeks to identify the timeframe required for each tasking request, and how the request will help to address the abovementioned high priority issues as relevant to the applicant sector or organisation. The principal criterion, 'criticality', is described at **Attachment C**.

2.1 The Tasking Request Process (Submission of Tasks)

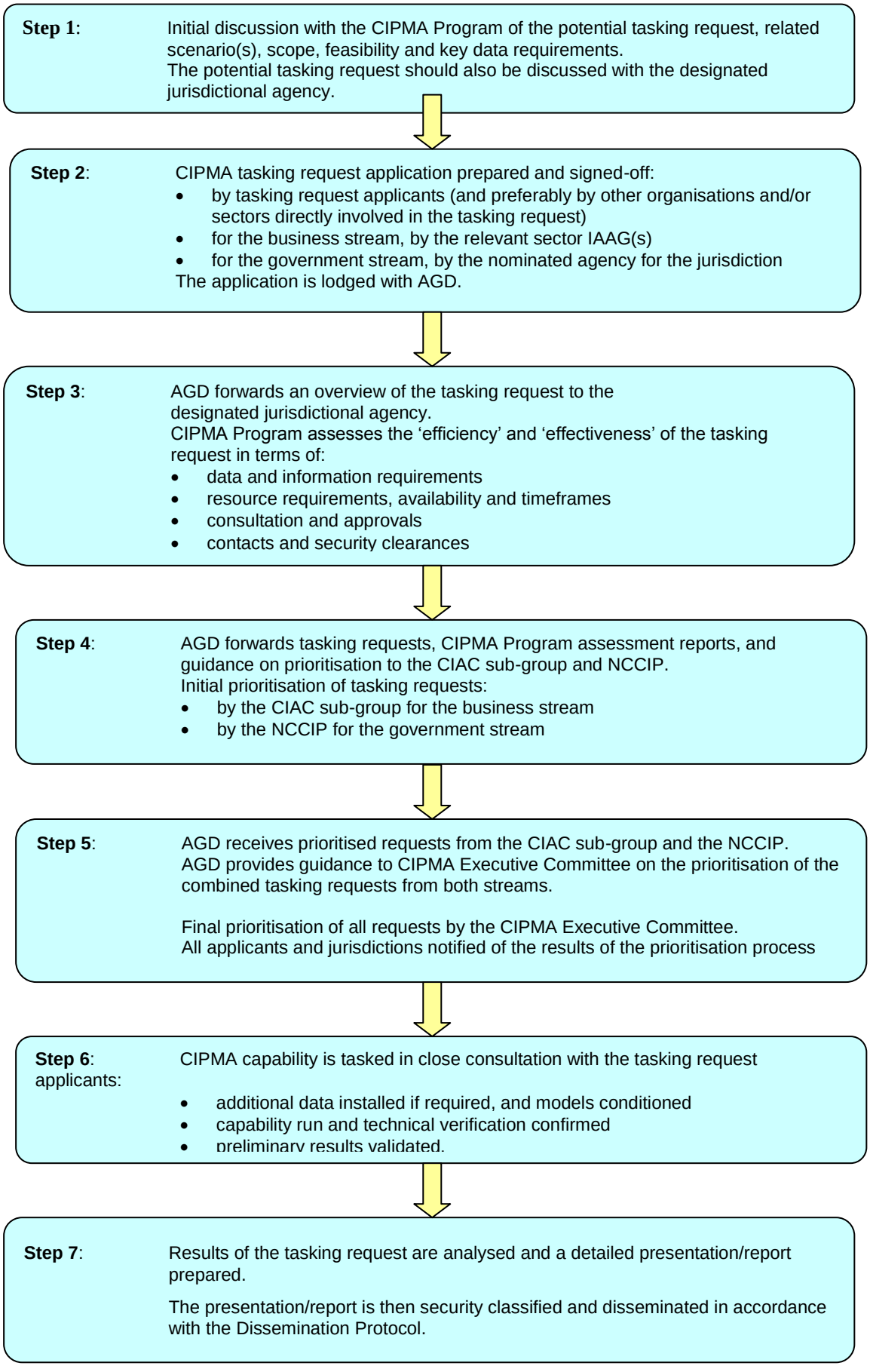
Tasking requests are submitted to AGD for approval and prioritisation, with Geoscience Australia performing the analysis.

A tasking request could originate from a range of organisations, including:

- an individual business or government business enterprise, or several of these business organisations working together
- a critical infrastructure sector, or a number of sectors, or
- a government organisation or several organisations within or across jurisdictions (Australian Government, State or Territory Government, and in some circumstances local government).

A two 'stream' process for tasking the CIPMA capability will operate; one stream for requests originated by business organisations and the other for government organisations. While there are some specific differences between the two streams, the generalised process for both streams is described in Figure 1 as follows.

Figure 1 Overview of the Tasking Request Process



2.2 Detailed Description of the Tasking Request Process

Step 1: ***Initial discussion with the CIPMA Program*** (Pre Application)

The tasking applicant(s) will initially meet with the CIPMA Program Manager to discuss the proposed tasking request. This early consultation with the CIPMA Program is to ensure that the tasking request is both realistic and broadly feasible given the level of development of the capability and the availability of key data sets. A data set is regarded as "available" if the data is already installed in the CIPMA capability or can be captured quickly and easily.

The contact point for initial discussions with the CIPMA Program is the CIPMA Project Officer 02 6141 2951 in the Critical Infrastructure Protection Branch, Attorney-General's Department.

State-Owned Corporations and Government Business Enterprises should discuss the proposed tasking request with the designated critical infrastructure protection agency in their jurisdiction before initial discussion with the CIPMA Program (see **Attachment D** for contact details in each jurisdiction).

All other applicants are encouraged to discuss tasking requests with the designated agency in their jurisdiction prior to lodging a tasking request application. Early consultation will enable the jurisdiction to consider co-sponsoring a tasking request.

Step 2: ***Completing and Lodging a Tasking Request Application***

Once the broad feasibility of the initial tasking request has been verified by the CIPMA Program, the applicant must complete a formal CIPMA tasking application form (see **Attachment E**) and lodge it with AGD. The completed application provides the CIPMA Program with more detailed information on the nature and scope of the refined tasking request and related scenario(s). Information required in the tasking request application includes the following:

- A reasonably detailed description of the scenario(s) the applicant is seeking to run on the capability. (As the level of detail required will vary from scenario to scenario, AGD is available to provide guidance in this matter).
- A succinct overview of the scenario (note: this overview will be copied to the designated jurisdictional agencies, as listed in Attachment D, for information. This is to ensure that all jurisdictions have broad visibility of all tasking requests and will enable any jurisdiction that has a particular interest in a request originating in their jurisdiction to contact the tasking applicant for discussion or to seek to co-sponsor the request).
- Confirmation that the organisations and/or industry sectors directly involved in the tasking request have been consulted and preferably have approved the use of their data for the request. For example, if the banking and finance sector wants to investigate dependencies on communications infrastructure in Sydney or Melbourne, the banking and finance sector should discuss this tasking request with the relevant communications carriers prior to the application stage. The preferred outcome would be that the communications carriers join the banking and finance sector as co-applicants in the tasking request, or otherwise provide written confirmation that they have been consulted about the proposed tasking request and agree to the use of their data. The CIPMA Program is able to assist by brokering initial contact between applicants and data owners if necessary.
- A business case detailing why the tasking request is important and how it addresses the primary criterion, 'criticality'. That is, how this work will assist with addressing the high priority issues of critical infrastructure protection, counter-terrorism and/or emergency management that are relevant to the applicant sector or organisation(s).

- The contact and security clearance details of the applicant(s) and the other participants identified in the application, and evidence that the request has the support of either the relevant sector Infrastructure Assurance Advisory Group (IAAG) (for business stream tasking requests) or the relevant jurisdictional agency (for government stream tasking requests).
- If applicants from the business stream are seeking a security clearance, the completed clearance request forms should also be attached to the application (see section 4 for more details on security clearances).

The complete tasking request application is to be lodged electronically in Word format with the CIPMA Program for registration. The application form is available from the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) website (www.tisn.gov.au). Closing dates for applications will be at the end of February, June and October each year (see Attachment A).

Step 3: ***Notification of the application and initial assessment by the CIPMA Program***

Upon receipt of the tasking request applications, AGD will forward the "scenario overview" and contact details of the tasking request applicants to all designated jurisdictional agencies. This will enable any State or Territory that has a particular interest in a tasking request to contact the proponent for further information, or to seek to co-sponsor the tasking request.

Initial assessment of tasking requests is undertaken by the CIPMA Program. The assessment will focus on 'efficiency' and 'effectiveness' (for example, will running this tasking request produce outcomes that constitute an efficient use of CIPMA resources and generate effective outcomes for the CIPMA Program). The CIPMA Program will seek to verify that:

- the CIPMA capability has the required data and information to run the tasking request
- the resources to condition the models and run the tasking request are available within the timeframes specified in the request or within an alternative timeframe acceptable to the tasking applicant, and
- the tasking request applicant has consulted with, and preferably obtained approval from, the owners of the data required to run the request.

If the assessment process finds there is insufficient data or information to run a tasking request, two options arise:

(i) the CIPMA Program may assist the applicant to obtain confirmation from the owner of the missing data/information so that the data would be made available at the appropriate time for use in CIPMA. The CIPMA Program would make an assessment of the resources and timeframes required to actually capture the missing data, or

(ii) the applicant may amend the tasking request to ensure that it can be run with data and information already installed in the CIPMA capability.

The CIPMA Program's assessment of the efficiency and effectiveness of the tasking request will be taken into account in the prioritisation process.

Step 4: ***Initial Prioritisation of Tasking Requests***

Once the tasking request clears the registration and initial assessment process, initial prioritisation is undertaken for requests within each stream (the business stream and the government stream).

AGD will forward the tasking request applications, the CIPMA Program's assessment of efficiency and effectiveness and guidance on prioritisation to the National Committee on Critical

Infrastructure Protection (NCCIP) for government stream requests or the sub-group of the Critical Infrastructure Advisory Committee (CIAC) for business stream requests.

The criterion of 'criticality' will apply to the initial prioritisation of tasking requests for both streams. Descriptors of 'criticality' are at Attachment C.

Business stream tasking requests: Initial prioritisation of business stream tasking requests is undertaken by a sub-group of the Critical Infrastructure Advisory Committee (CIAC). The sub-group will be comprised of CIAC members who represent the Infrastructure Assurance Advisory Groups (IAAGs) that are engaged in CIPMA and where coverage of these sectors is sufficiently advanced to allow tasking (currently banking and finance, communications, energy, water and transport). Further information about the CIAC can be found at **Attachment F**.

The designated jurisdictional agency listed in Attachment C will have the choice of utilising either the business or the government stream for requests from State-Owned Corporations and Government Business Enterprises.

Government stream tasking requests: Initial prioritisation of government stream tasking requests will be undertaken by the National Committee on Critical Infrastructure Protection (NCCIP). NCCIP is a formal standing committee established to coordinate CIP policy development across all levels of government. Further information about the NCCIP can be found at Attachment F.

NCCIP and the CIAC sub-committee will assess the applications received and forward their prioritised lists to AGD.

Step 5: ***Final Prioritisation of Tasking Request Applications***

Final prioritisation will take place when the ranked requests from the two separate streams come together and final priorities are allocated across the business and government streams. Responsibility for assigning final prioritisation will rest with the CIPMA Executive Committee which comprises four members from the Australian Government: the Chair of CIAC and a representative each from the National Counter-Terrorism Committee (NCTC), the Australian Emergency Management Committee (AEMC) and the Australian Security Intelligence Organisation (ASIO).

AGD will forward the tasking request applications, the initial prioritisations from the CIAC sub-group and the NCCIP, the CIPMA Program's assessment of efficiency and effectiveness and guidance on prioritisation to the CIPMA Executive Committee to assist its deliberations on final prioritisation.

Final prioritisation will be determined using the same criterion of criticality and will take account of the CIPMA Program's assessment of the 'efficiency' and 'effectiveness' of each request.

Following the final prioritisation of tasking requests by the Executive Committee, AGD will advise all applicants and jurisdictions of the outcome, and arrange meetings with successful applicants to clarify and agree to the task scope, data required and timeframe. Following the meeting the prioritised tasking requests will be forwarded to the CIPMA Program for running on the CIPMA capability.

Any data received after the agreed deadline, and any additional work to be added to the previously agreed scope may result in a delay in the finalisation of the task.

Approved tasking requests may not be able to commence until agreement is reached to a new end of task date.

Step 6: ***Running the Prioritised Tasking Requests on the CIPMA Capability***

The CIPMA Program will work with the tasking request applicants to run the request on the CIPMA capability. The steps involved in running a request will include:

- acquiring and/or loading any additional data required to run the request
- conditioning the models to align with the parameters of the request
- running the tasking request and related scenario(s)
- verifying the run process, and
- initial validation of results.

Technical Verification and Initial Validation of Results: The preliminary results of the tasking request will be verified by the CIPMA Program to ensure the CIPMA capability successfully executed all of the phases of the run process. Specifically, the CIPMA Program will undertake an error check to ensure that all relevant capability processes were executed in accordance with CIPMA architecture and technical procedures.

If required, the capability may be fine-tuned and the request re-run until technical verification is confirmed.

Step 7: ***Analysis of Results and Preparation of the Presentation/Report***

The CIPMA Program will analyse the results from a tasking request and prepare a detailed presentation/report of the findings of the analysis.

The main visualisation tool in the CIPMA capability is the Geospatial Information System (GIS). The presentation/report prepared by the CIPMA Program will use the GIS to present the results and subsequent analysis. The presentation/report may also use a number of other tools such as Microsoft PowerPoint.

Once the analysis of results and presentation/report is prepared, the tasking process is complete and the dissemination process commences.

2.2.1 *Urgent Tasking Requests*

If there is an urgent requirement to task the CIPMA capability in response to an actual or imminent event, the Deputy Secretary, National Security and Criminal Justice, AGD (as Chair of CIAC and the CIPMA Executive Committee) may allocate priority to a tasking request as considered appropriate. In these circumstances the need to adhere to the prioritisation steps in this protocol will be suspended.

3. The Dissemination Protocol

The dissemination protocol has been developed to ensure the appropriate and secure dissemination of tasking results, and to safeguard the integrity and confidentiality of the data and models.

3.1 The Dissemination Process

The dissemination process commences following an analysis of results from the tasking request and the completion of the presentation/report.

The dissemination process contains three steps.

1. AGD will classify the presentation/report in accordance with the *Protective Security Manual 2005* (Cth.) ('PSM').
2. The presentation/report will be disseminated to the tasking request applicants and any co-applicants who hold an appropriate security clearance*, satisfy the "need-to-know"* principle and satisfy any physical security standards required by the TISN Deed of Agreement.
3. A sanitised* IN-CONFIDENCE level overview report will be prepared by AGD **in consultation with the tasking applicants**, and will be forwarded to the designated agency in all jurisdictions for information. This is to ensure that all jurisdictions have broad visibility of the generalised findings from CIPMA.

3.1.1 *Classification of the Presentation/Report:*

AGD will classify the presentation/report in accordance with the PSM. The classification and any additional caveat will be applied on a case-by-case basis. Guidance on the classification process is at **Attachment G**.

It is expected the minimum classification of a presentation/report will be PROTECTED. In some cases, a presentation/report may contain information that has national security* significance, at either the CONFIDENTIAL or SECRET level. Where this occurs, the presentation/report will carry a national security classification in accordance with the PSM.

The type and level of classification of a presentation/report will determine how this information is to be managed and stored, and who is authorised to have access to the information, subject to the "need-to-know" principle.

3.1.2 *Dissemination of the Classified Presentation/Report:*

The dissemination of results from running the tasking request in the CIPMA capability will generally take the form of a detailed briefing to the tasking request applicant(s) and, where agreed by the applicant, to other stakeholders. The detailed briefing will take place in the applicant's organisation or in the CIPMA secure facility in Canberra.

Prior to the briefing, AGD will confirm the details of the security clearances held by attendees to ensure that they are current and appropriate for the classification of the presentation/report being presented at the briefing.

Electronic copies of a presentation/report will not be made available to briefing attendees for the foreseeable future.

* See Attachment B for an explanation of these terms.

A hard copy of the presentation/report will be made available to briefing attendees subject to conditions in the TISN Deed of Agreement being satisfied.

The Deed requires personnel who access security classified information to have an appropriate security clearance. The Deed provides for AGD, in appropriate circumstances, to sponsor and arrange security clearances for personnel responsible for dealing with the information.

In addition, AGD will prepare a sanitised IN-CONFIDENCE version for distribution, upon request, to relevant staff within tasking applicant organisations, who do not hold a security clearance but have a demonstrated "need-to-know". AGD will consult with applicant organisations with regard to the contents of this sanitised report.

AGD recognises that, in certain circumstances, the senior executives from applicant organisations may need to receive a detailed briefing (above the IN-CONFIDENCE level) on the key findings of a presentation/report. AGD will consider these requests on a case by case basis and may agree to these requests subject to certain conditions being met.

Further information on security clearances and physical security requirements is detailed in Section 4 of this document.

3.1.3 *Provision of a sanitised report to State and Territory Jurisdictions*:

A sanitised* IN-CONFIDENCE level overview report will be prepared by AGD **in consultation with the tasking applicants**, and will be forwarded to the designated agency in all jurisdictions for information. This is to ensure that all jurisdictions have broad visibility of the generalised findings from CIPMA.

3.1.4 *"Exceptional Circumstances" requests from State and Territory Jurisdictions for provision of a full report:*

In exceptional circumstances, a designated jurisdictional agency may request a hard copy of the detailed presentation/report of a tasking application where that jurisdiction was not a co-applicant in the tasking process.

This request must be made in writing to AGD and forwarded to the CIPMA Project Officer. Each request will be assessed by both AGD and the tasking applicant(s).

Requests can only be considered if, based on information contained in the sanitised IN-CONFIDENCE report provided to the jurisdiction, the full report/presentation is likely to include substantive analysis of significant infrastructure located in that jurisdiction. The request should also address:

- the specific reasons, in addition to the above minimum requirement, for requiring the full presentation/report
- the reasons why the jurisdiction did not participate in the tasking process as a co-applicant, and
- clear evidence of a "need-to-know".

The detailed presentation/report will only be released to a designated jurisdictional agency with the agreement of all tasking applicant(s).

4. Safeguarding Security Classified Information

4.1 Security Clearance Requirements

In normal circumstances, an individual will need to possess an appropriate security clearance to receive the detailed and sensitive results of a tasking request, whether in the form of a briefing in or related hard copy.

A CIPMA presentation/report could contain information that has national security significance up to the SECRET level. AGD recognises that applicant organisations from the business stream may not have employee(s) who hold a current security clearance at the SECRET level. In these circumstances, the following arrangements will apply:

- AGD will sponsor up to two employees from the organisation to obtain a SECRET level clearance
- as it can sometimes take several months to obtain a SECRET level security clearance, business stream organisations planning to task the CIPMA capability should begin the process of obtaining security clearances for required personnel when tasking request applications are lodged, and
- the process may be initiated by the organisation completing a 'Request for Security Clearance form' found at **Attachment H.** This form is also available from the TISN website.

While AGD will sponsor up to two employees from a business stream organisation to obtain a SECRET level clearance, the cost of the clearance must be borne by the business. Currently the cost of obtaining a SECRET level clearance is less than $1,000 per person. Further information on the security clearance process may be obtained from the CIPMA Project Officer.

If the general results of a tasking request need to be distributed to people within an organisation who have a "need-to-know" but do not hold the appropriate national security clearance (e.g. SECRET), AGD will prepare an IN-CONFIDENCE classified level report to facilitate a broader distribution process. It is the responsibility of each organisation (business or government) to ensure that uncleared personnel do not have access to CIPMA related information and results classified above IN-CONFIDENCE.

Note that national classified information (e.g. SECRET) cannot be shared with those who do not hold a national security clearance, even if they have a valid 'need-to-know'.

Receivers of national security classified information must have the proper clearances in order to receive such information. National security classified information, that is information marked as TOP SECRET, SECRET, or CONFIDENTIAL, must only be given to a person who holds a valid, current, security clearance at an equivalent or higher level that the information being provided.

As stated in section 3.1.2, AGD recognises that, in certain circumstances, the senior executives from applicant organisations may need to receive a detailed briefing (above the IN-CONFIDENCE level) on the key findings of a presentation/report. AGD will consider these requests on a case by case basis and may agree to these requests subject to certain conditions being met.

4.2 Physical Security Requirements

The TISN Deed of Agreement covers the responsibilities and obligations for safeguarding classified information. Essentially, the Deed requires organisations to adhere to the policies set out in the PSM when dealing with security classified material. The PSM sets minimum standards for storing

security classified information that apply to electronic information systems and physical storage facilities.

Business stream organisations will be required to sign a TISN Deed of Agreement prior to receiving hard copies of CIPMA security classified reports.

As outlays associated with meeting physical security conditions relate to property and equipment owned by organisations themselves, the relevant organisation is responsible for meeting these costs.

Further information on the requirements of the Deed and physical security conditions may be obtained from the CIPMA Project Officer.

Attachment A: Indicative schedule for the tasking application prioritisation process

Step 1 Discussions with the CIPMA Program /designated Jurisdictional agency/ IAAG on proposed request	
Step 2 Request applications close at the end of the listed months each year	February, June and October each calendar year
Step 3 Registration of applications and provision of overview and contact details to designated jurisdictional agency	Completed within 1 week of closure of tasking round
Initial assessment by CIPMA Program (undertaken in consultation with applicants)	Completed within 2 weeks of closure of tasking round
Step 4 AGD groups applications into either business or government streams, prepares guidance advice, and forwards requests and advice to the NCCIP (government stream) and CIAC sub-committee (business stream) for initial prioritisation	Completed within 3 weeks of closure of tasking round
NCCIP and CIAC sub committee complete initial prioritisation and forward prioritised list to AGD	Completed within 4 weeks of closure of tasking round
Step 5 AGD forwards advice to CIPMA Executive Committee on final prioritisation of all requests for final prioritisation	Completed within 5 weeks of closure of tasking round
CIPMA Executive Committee completes the final prioritisation of tasking requests. All applicants and designated jurisdictional agencies notified of results of prioritisation process	Completed within 6 weeks of closure of tasking round

Attachment B: Glossaries

Abbreviations and Acronyms

AGD	Attorney-General's Department (Cth.)
ASIO	Australian Security Intelligence Organisation
CIPMA PROGRAM	The CIPMA Program is managed and funded by AGD, with GA is engaged as the lead technical provider.
CIAC	Critical Infrastructure Advisory Council
CIP	Critical Infrastructure Protection
CIPMA	Critical Infrastructure Protection Modelling and Analysis Program
EAG	Expert Advisory Group
GA	Geoscience Australia
GIS	Geospatial Information System
IAAG	Infrastructure Assurance Advisory Group
NCCIP	National Committee for Critical Infrastructure Protection
NCTC	National Counter-Terrorism Committee
PSM	Protective Security Manual 2005 (Cth.)

Security Classifications

National Security Classifications	
TOP SECRET	A protective marking that shows that compromise of the official information could cause exceptionally grave damage to national security
SECRET	A protective marking that shows that compromise of the official information could cause serious damage to national security
CONFIDENTIAL	A protective marking that shows that the compromise of the official information could cause damage to national security
RESTRICTED	A protective marking that shows that the compromise of the official information could cause limited damage to national security
UNCLASSIFIED	Unclassified information – official information that is not security classified; it may be unlabelled or it may be marked UNCLASSIFIED

Non-National Security Classifications	
HIGHLY PROTECTED	A non-national security protective security marking that shows that compromise of the official information could cause serious damage to Australia, the Australian Government, commercial entities or members of the public
PROTECTED	A non-national security protective marking that shows that compromise of the official information could cause damage to Australia, the Australian Government, commercial entities or members of the public
"X"-IN-CONFIDENCE	A non-national security protective marking that shows that compromise of the official information could cause limited damage to Australia, the Australian Government, commercial entities or members of the public. "X" will be replaced by a designation such as "Commercial", "TISN", "Security" or similar.

Terminology

Clearance (process)	In the context of personnel security clearances, the process of assessing a person's suitability for access to security classified information.
Harm	Any negative consequence, such as compromise of, or damage to, or loss incurred by, the Australian Government or commercial entity.
National Security	A term used to describe the safety of the nation from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system or acts of foreign interference.
(National) Security Clearance	A clearance a person must hold before he or she can access national security information classified at CONFIDENTIAL, SECRET or TOP SECRET.
'Need-to-know' principle	The principle that the availability of official information should be limited to those who need to use or access the information to do their work.

Sanitised	A document that has been through a process where certain elements of information have been removed to allow the protective marking that indicates the level of protection required for security classified information to be removed or reduced – this can refer to both electronic media and hard copy information.
Security Classification (System)	A set of procedures for identifying official information whose compromise could have adverse consequences for the Australian Government – it is the Government's mechanism for protecting the confidentiality of information generated by it or provided to it by other governments and private entities; the security classification system is implemented by assigning protective markings (such as TOP SECRET, PROTECTED, etc); the protective marking not only shows the value of the information but also indicates the minimum level of protection it must be afforded to safeguard it from compromise.

Attachment C: 'Criticality' criterion - description

Critical infrastructure is defined as 'those physical facilities, supply chains, information technologies and communication networks that, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation or affect Australia's ability to conduct national defence and ensure national security'.

CIPMA supports decision making by helping to:

- identify connections between critical infrastructure nodes and facilities within sectors and across sectors
- provide insights into the behaviour of complex networks
- analyse relationships and dependencies
- examine the flow-on effects of infrastructure failure
- identify choke points, single points of failure and other vulnerabilities
- assess various options for investment in security measures, and
- test mitigation strategies and business continuity plans.

'Criticality' will be the primary criterion by which tasking requests will be assessed and prioritised. That is, how the request will help address the high priority issues of critical infrastructure protection, counter-terrorism and/or emergency management that are relevant to the applicant sector or organisation.

In prioritising tasking requests the CIPMA Executive Committee will take account of the ranking of requests by the CIAC sub-group and the NCCIP.

The CIPMA Executive Committee will also take account of the CIPMA Program's assessment of 'efficiency' and 'effectiveness'. That is, to what extent will running a tasking request produce outcomes that:

- constitute an efficient use of CIPMA resources, such as the data, resources and time needed to run the scenario, and
- generate effective outcomes for the CIPMA Program (eg the best results possible to meet the reasonable expectations of the tasking organisation, CIPMA stakeholders and CIPMA objectives generally).

Completing question 4 of the tasking application form

In responding to the issue of criticality applicants could include comment on the consequences of failure/unavailability of the asset including the

- impact on a key business process
- impact on the organisation, their customers and the community
- availability of redundancies or alternatives
- capability and time taken to resume acceptable service levels, recover capability, or resume normal operations, and
- any pertinent reference in the applicant sector or organisation's disaster recovery plan, business continuity plan, risk management plan or similar.

Further guidance on criticality may be found in the *Critical Infrastructure Protection Risk Management Framework for the Identification and Prioritisation of Critical Infrastructure* and *Handbook 167:2006 to the AS/NZS 4360: 2004 Risk Management Standard.*

Attachment D: Government Critical Infrastructure Protection Coordinator Contact Details

Australian Government		
CIPMA Project Officer Modelling and Analysis Critical Infrastructure Protection Branch Attorney-General's Department	Tel Email	(02) 6141 2951 cipprojects@ag.gov.au

Australian Capital Territory		
Mr James Henry Senior Director Security and Emergency Management Branch ACT Department of Justice and Community Safety	Tel Fax Email Mail	(02) 6205 5132 (02) 6249 1730 james.henry@act.gov.au Level 9, 12 Moore St CANBERRA CITY ACT 2601

New South Wales		
Director Counter Terrorism and Disaster Recovery NSW Department of Premier & Cabinet	Tel Fax Email Mail	(02) 8374 5132 (02) 8374 5184 CTDR@dpc.nsw.gov.au GPO Box 5341 SYDNEY NSW 2001

Northern Territory		
Security Coordinator Security & Emergency Recovery Northern Territory Government Department of the Chief Minister	Tel Fax Email Mail	(08) 8999 8971 (08) 8999 7402 beth.moloney@nt.gov.au GPO Box 4396 DARWIN NT 0801

Queensland		
Security Planning and Coordination Department of the Premier and Cabinet	Tel Fax Email Mail	(07) 3238 3643 (07) 3224 2089 Security@premiers.qld.gov.au PO Box 15185 CITY EAST QLD 4002

South Australia		
South Australia Police Sgt Alistair Robertson Sgt Kev Carroll Sgt John Hood	Email Tel Tel Tel	Sapol.sacis@police.sa.gov.au (08) 8207 4026 (08) 8207 4618 (08) 8207 4683

Tasmania		
Mr Simon Roberts State Security Unit Department of Police and Emergency Services	Tel Email Mail	(03) 6230 2500 simon.roberts@police.tas.gov.au GPO Box 308C HOBART TAS 7001

Victoria		
Mr Bruce Pickthall Project Officer Security and Emergencies Unit Department of Premier and Cabinet	Email Tel	bruce.pickthall@dpc.vic.gov.au
Ms Jo Tan	Email	jo.tan@dpc.vic.gov.au
Mr Peter Mason Manager Security and Emergencies Preparedness Department of Premier and Cabinet	Email Tel	peter.mason@dpc.vic.gov.au (03) 9651 1042

Western Australia		
Manager Office of State Security and Emergency Coordination Department of the Premier and Cabinet	Tel Fax Email Mail	(08) 9222 9303 (08) 9322 2367 ossec@dpc.wa.gov.au 197 St George's Terrace PERTH WA 6000

Attachment E

Australian Government

Attorney-General's Department

Security and Critical
Infrastructure Division

Critical Infrastructure Protection Modelling and Analysis (CIPMA) Program

Tasking Application Form

This form seeks information on the applicant organisation(s), organisation contact officer(s), proposed recipients of the tasking results, a description of the proposed scenario and a statement in response to the criterion of criticality.

All information provided in completing this form will be treated as "COMMERCIAL-IN-CONFIDENCE" once the completed application is received by the Attorney-General's Department.

Questions about the completion of the tasking application form should be directed to cipprojects@ag.gov.au or telephone 02 6141 2951

Completed applications must be lodged electronically with:

CIPMA Project Officer
Modelling and Analysis
Critical Infrastructure Protection Branch
Attorney-General's Department
cipprojects@ag.gov.au

1. Applicant Organisation(s)

(i) Lead Applicant Organisation

Organisation Name				
Type of organisation	Business		Government Business Enterprise	
	Government Agency		State-Owned Corporation	
'Stream' nomination	Business		Government	
	You should note that the type of organisation will determine in which 'stream' (government or business) the tasking application will be processed: *(i) Government departments/agencies should nominate the 'government' stream.* *(ii) with the agreement of the designated jurisdictional agency, Government Business Enterprises/State-Owned Corporations may elect either the 'business' or 'government' stream.* *(iii) where a tasking application is being co-sponsored by organisations from both 'business' and 'government' the designated stream will correspond to that of the organisation designated as the 'Lead Applicant Organisation'.* *(iv) tasking applications from government stream organisations must have the support of the designated jurisdictional agency (see Attachment C to the Tasking and Dissemination Protocols for jurisdiction contact details)* *(v) tasking applications from business stream organisations must have consulted with their relevant sector Infrastructure Assurance Advisory Group.*			

Lead Applicant Organisation Primary Contact Person*	Title	
	First Name	
	Surname	
	Position	
	Phone	
	Fax	
	Email	
	Security clearance** *(if held)*	
	*Please provide the details of a primary and secondary contact person for each organisation that is sponsoring the tasking application. **Please provide details of any security clearance currently or previously held, including level, date of issue and issuing agency. *You should note that:* *(i) where more than one organisation is sponsoring a tasking application, the contact person for the 'Lead Applicant Organisation' will be the primary point of contact.* *(ii) the lack of a current or previous security clearance will not disadvantage the assessment of a tasking application. Please refer to Section 4 of the CIPMA Tasking and Dissemination Protocols for information on the process to request a security clearance.*	

Lead Applicant Organisation Secondary Contact Person	Title	
	First Name	
	Surname	
	Position	
	Phone	
	Fax	
	Email	
	Security clearance *(if held)*	

(ii) Co-Applicant Organisation(s) (if applicable)					
Organisation Name					
	Please provide details of any co-applicant organisation and its contact officer. *You should note that all Co-Applicant Organisations will receive the full results of the tasking request subject to meeting security clearance requirements.*				
Type of organisation	Business		Government Business Enterprise		
	Government Agency		State-Owned Corporation		
Primary Contact Person	Title				
	First Name				
	Surname				
	Position				
	Phone				
	Fax				
	Email				
	Security clearance *(if held)*				
Secondary Contact Person	Title				
	First Name				
	Surname				
	Position				
	Phone				
	Fax				
	Email				
	Security clearance *(if held*)				

2. Recipients of Results

Please provide details of any organisation(s), other than those listed at Q1 above, that should receive the results of the tasking request (subject to security clearance requirements).

Organisation Name		
Contact Person	Title	
	First Name	
	Surname	
	Position	
	Phone	
	Fax	
	Email	
	Security clearance* *(if held)*	
	*Please provide details of any security clearance currently or previously held, including level, date of issue and issuing agency. *You should note that the lack of a current or previous security clearance will not disadvantage the assessment of a tasking application.*	
Organisation Name		
Contact Person	Title	
	First Name	
	Surname	
	Position	
	Phone	
	Fax	
	Email	
	Security clearance *(if held)*	

3. Scope

a. Scenario Overview

Please provide a brief overview description of the proposed scenario.

You should note that this overview and the proponent's contact details will be forwarded to the designated jurisdictional agency for information. This will enable any state/territory that has a particular interest in a tasking request to contact the proponent for further information, or seek to co-sponsor the tasking request.

Answer (Maximum 150 words)

b. Scenario Description

Please provide a more detailed description of the proposed tasking request.

The scenario description could include details of:

- *the physical facilities, supply chains, information technologies and communication networks*
- *the scenario 'event', that may result in the destruction, degradation or rendered unavailable for an extended period*
- *the estimated impact on the social or economic well-being of the nation or estimated affect on Australia's ability to conduct national defence and ensure national security*
- *the affected critical infrastructure nodes and facilities within sectors and across sectors*
- *any existing identified choke points, single points of failure and other vulnerabilities that may be affected by the scenario event*
- *any existing mitigation strategies or business continuity plans that will be tested*
- *the benefits for each organisation intended to receive the results, and*
- *any other relevant information.*

Answer (Maximum 500 words)

4. Response to 'criticality' criterion

Critical infrastructure is defined as 'those physical facilities, supply chains, information technologies and communication networks that, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation or affect Australia's ability to conduct national defence and ensure national security'.

CIPMA supports decision making by helping to:

- identify connections between critical infrastructure nodes and facilities within sectors and across sectors
- provide insights into the behaviour of complex networks
- analyse relationships and dependencies
- examine the flow-on effects of infrastructure failure
- identify choke points, single points of failure and other vulnerabilities
- assess various options for investment in security measures, and
- test mitigation strategies and business continuity plans.

'Criticality' will be the primary criterion by which tasking requests will be assessed and prioritised. That is, how the request will help address the high priority issues of critical infrastructure protection, counter-terrorism and/or emergency management that are relevant to the applicant sector or organisation.

In prioritising tasking requests the CIPMA Executive Committee will take account of the ranking of requests by the CIAC sub-group and the NCCIP.

The CIPMA Executive Committee will also take account of the CIPMA Program's assessment of 'efficiency' and 'effectiveness'. That is, to what extent will running a tasking request produce outcomes that:

- constitute an efficient use of CIPMA resources, such as the data, resources and time needed to run the scenario, and
- generate effective outcomes for the CIPMA Program (eg the best results possible to meet the reasonable expectations of the tasking organisation, CIPMA stakeholders and CIPMA objectives generally).

Completing question 4 of the tasking application form

In responding to the issue of criticality applicants could include comment on the consequences of failure/unavailability of the asset including the

- impact on a key business process
- impact on the organisation, their customers and the community
- availability of redundancies or alternatives
- capability and time taken to resume acceptable service levels, recover capability, or resume normal operations, and
- any pertinent reference in the applicant sector or organisation's disaster recovery plan, business continuity plan, risk management plan or similar.

Further guidance on criticality may be found in the *Critical Infrastructure Protection Risk Management Framework for the Identification and Prioritisation of Critical Infrastructure* and *Handbook 167:2006 to the AS/NZS 4360: 2004 Risk Management Standard.*

Answer (Maximum 300 words)

5. Consultation

Please provide advice on all relevant organisations/agencies that have been consulted regarding the tasking request.

Please note that:
(i) consultation with your designated jurisdictional agency prior to formal submission of the application is mandatory if the lead organisation is a Government agency, Government Business Enterprise or State-Owned Corporation.
(ii) consultation with your designated jurisdictional agency prior to formal submission of the application is highly recommended for all other applicants.
(iii) any tasking application, regardless of nominated 'stream', that seeks to analyse sector data in detail must be discussed with that sector's Infrastructure Assurance Advisory Group for comment prior to lodging the application.
(iv) data owners must be consulted and approve the use of their data. The CIPMA Program is able to broker initial contact between initial applicants and data owners if this has not already occurred.

Please indicate whether consultation with the following bodies has been conducted:

Yes	**No**	
		a. the CIPMA Program
		b. your sector Infrastructure Assurance Advisory Group (IAAG)
		c. any other sector IAAG – if YES, please specify -
		d. your designated jurisdictional agency (mandatory for Government stream tasking requests)
		e. the owners of the required data and information
		f. if the answer to (e) is yes, and the data owners are not co-applicants, have the owners agreed to the use of their data for this tasking request?
		g. any organisation named in your answer to Q 2 above
		h. any other agency/organisation?

6. Time-frame for dissemination of tasking request results

Please provide details of any preferred time-frame for the tasking request to be run and results to be made available or how the time-frame might relate to other factors, events or decisions to be taken in the tasking organisation.

Please note that:
(i) the results of some tasking applications may need to be available to enable timely input to other planning or procurement processes in the lead or co-applicant organisation. However the lack of any specific preferred time frame will not disadvantage a proposed tasking request.
(ii) to maximise value from the results of the tasking process it is important that the environment in which the infrastructure is operating is relatively stable, with no significant changes planned for the near future that would quickly nullify the results of the tasking application.

Please advise any preferred date for the results of the tasking process to be available, and any reasons/factors/issues etc that are relevant to the preferred date:

a. any specific preferred date

b. any relevant critical operational factors eg any impact on planned infrastructure purchases/upgrades/replacements etc

c. stability of the environment

d. any adverse impact if the preferred date is not met

Attachment F: CIAC and NCCIP

Critical Infrastructure Advisory Council (CIAC) – overview

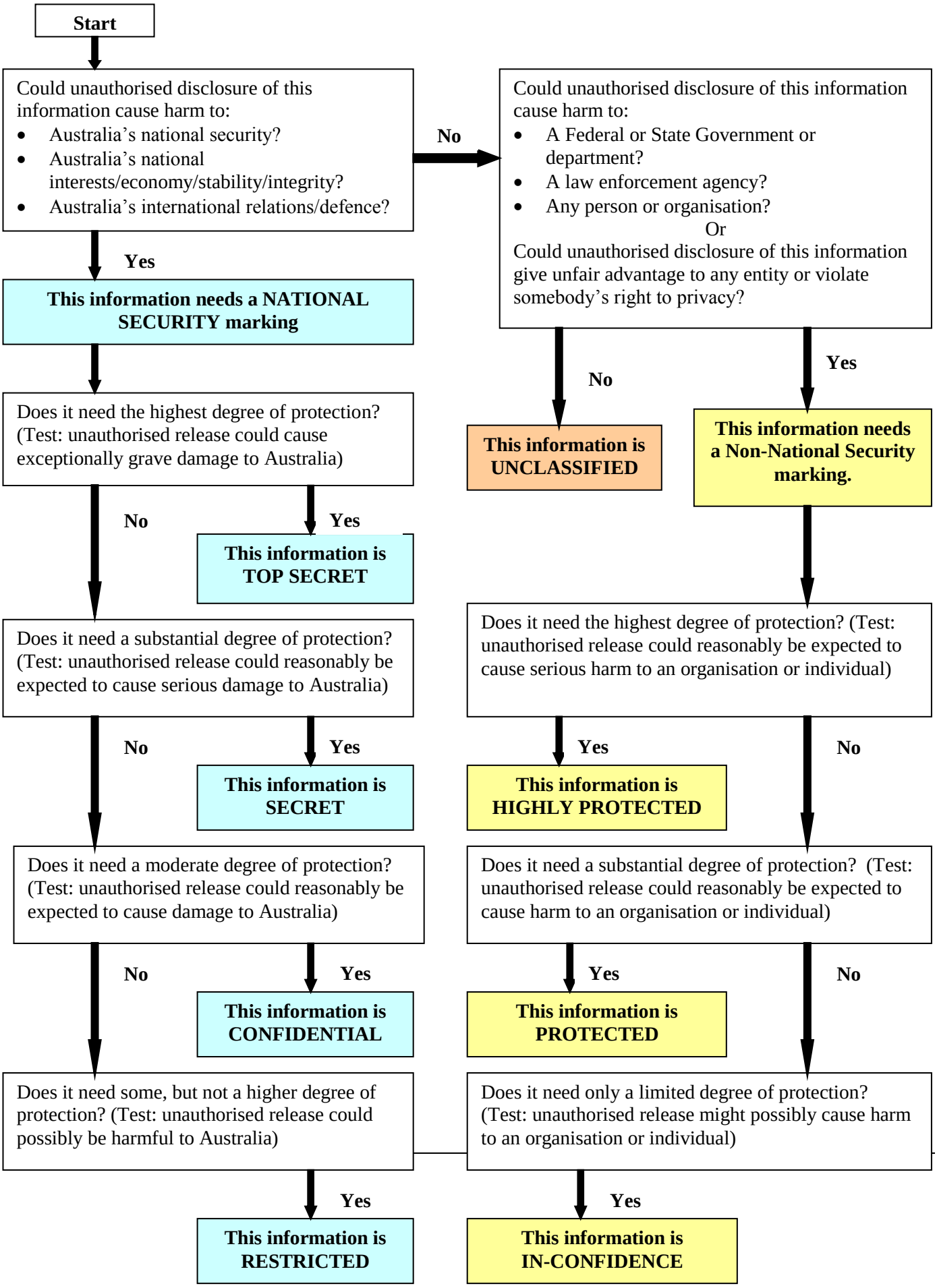
The Critical Infrastructure Advisory Council (CIAC) oversees the Infrastructure Assurance Advisory Groups (IAAGs) and advises the Attorney-General on the national approach to critical infrastructure protection. Established in August 2003, the Council draws its members from each of the nine sector advisory groups, each of the States and Territories, relevant Australian Government agencies and the National Counter-Terrorism Committee. It is chaired by the Attorney-General's Department, which also provides secretariat support.

Initial prioritisation of business stream tasking requests is undertaken by a sub-group of the CIAC. The sub-group will be comprised of CIAC members who represent the Infrastructure Assurance Advisory Groups (IAAGs) that are engaged in CIPMA and where coverage of these sectors is sufficiently advanced to all tasking (currently banking and finance, communications and energy).

National Committee on Critical Infrastructure Protection (NCCIP) – overview

The National Committee for Critical Infrastructure Protection (NCCIP) is a consultative forum which facilitates a whole-of-government approach to critical infrastructure protection and the subsequent maintenance of those services. The NCCIP provides an opportunity for the coordination and development of a nationally consistent, all-hazards approach to the protection of critical infrastructure. The NCCIP provides a policy coordination role, and does not have any operational role or purpose. It is chaired by the Attorney-General's Department, and comprised of representatives from a number of Commonwealth agencies, State and Territory First Minister's Departments, State and Territory Police, the Australian Local Government Association and a representative of the National Counter-Terrorism Committee (NCTC).

Attachment G: How to Select an Appropriate Security Classification



Australian Government
Attorney-General's Department

Protective Security
Coordination Centre

Security Clearance Request Form

This form is to request the assessment of a person's security clearance prior to their commencement at the department. This form is to be completed and forwarded to the Departmental Security Unit (DSU) for all people wishing to have access to the department or AGNET. It is in your interest to complete this form and forward it to the DSU as soon as possible as non-cleared personnel will not be able to start until they have received clearance from the DSU. **For help contact security on x6161 or press F1 on each field.** *All fields **MUST** be completed if applicable. All applicants **MUST** be Australian citizens.

Personal Details			
Surname:	**Given Names:**		
Previous Names:		**DOB:**	**POB:**
Email address:			
Phone no (BH):	**Phone no (mob):**		
Home address:			**Postcode:**
Australian Citizen YES ☐ NO ☐			
Previous/Current Employment Details			
Current Place(s) of Employment:			**AGS No**
Has this person held a security clearance? **Select one option only...**			**Level: Select option from list...**
Granted by:			**Grant Date:**
Has the Consent to Release Form been signed? **Select one option only...** **Consent form is located on Page two of this document**			
Vacancy Details			
Staff Type: **Select option from list...**	**Position Number:**		**Level: Select option from list...**
Proposed Start Date:	**End Date:**		**Position Title:**
Division:	**Branch:**		**Section:**
Security Clearance Required: **Select option from list...** **(Listing of DSAP and POT positions can be found on the Security Intranet site.)**			
Justification for Clearance : **(this section is only to be completed if a clearance level above the designated DSAP or POT position is required)**			
Requesting Officer	**Name:**	**Designation:**	
Branch:		**Phone No:**	**Date:**
Approving Officer (must be Director or above) Approved: YES ☐ NO ☐			
Name:		**Designation:**	
Division / Branch:		**Phone No:**	**Date:**
Upon completion of the Security Clearance Request Form, the Requesting Officer is to forward the form for approval to their Director or above, who on forwards it to the DSU mailbox at dsu@ag.gov.au for action.			

Security-in-Confidence
(after first entry)

Australian Government
Attorney-General's Department

Protective Security
Coordination Centre

Security Clearance Request Form

THIS FORM IS ONLY REQUIRED IF THE APPLICANT HAS BEEN GRANTED A CLEARANCE AND THEIR SECURITY FILE IS HELD BY ANOTHER AGENCY.

I hereby consent to the release of my Personal Security File to the Departmental Security Unit to enable the agency to assess my security status in accordance with its requirements.

Applicant

Full Name

Date of Birth

Signature .....

Date

Witness

Full Name

Signature .....

Date

Please forward completed 'Consent to the Release of Personal Security File' Form to the DSU by Fax to 02 6273 4041 or mail to the address below.

Departmental Security Unit
Attorney-General's Department
Protective Security Coordination Centre
10-12 Brisbane Avenue
BARTON ACT 2600