

Title: Competent PRS Authority IA No: Lead department or agency: UK Space Agency Other departments or agencies:	Impact Assessment (IA)
	Date: 13/06/2012
	Stage: Consultation
	Source of intervention: EU
	Type of measure: Secondary legislation
Contact for enquiries: Pete Lindsay peter.lindsay@ukspaceagency.bis.gsi.gov.uk; 020 7215 3728.	
Summary: Intervention and Options	RPC Opinion: Awaiting Scrutiny

Cost of Preferred (or more likely) Option				
Total Net Present Value	Business Net Present Value	Net cost to business per year (EANCB on 2009 prices)	In scope of One-In, One-Out?	Measure qualifies as
£-5.148m	£n/k	£0	No	NA

What is the problem under consideration? Why is government intervention necessary?
 Galileo, the satellite navigation system currently being built by the European Union and the European Space Agency will offer a number of services, one of which will be the Public Regulated Service (PRS). PRS will be restricted to government-authorized users. The government must intervene by creating a Competent PRS Authority (CPA) to authorize and monitor the use and manufacture of PRS technology due to regulatory failure. Without setting up a CPA the UK may not access PRS, nor may UK manufacturers make PRS technology according to the provisions of Decision 1104/2011/EU.

What are the policy objectives and the intended effects?
 The objective of the policy is to create the authorisation capability for PRS use and for PRS technology manufacture in the UK as well as to create a monitoring and enforcement capability to ensure compliance with PRS common minimum standards among PRS users and PRS technology manufacturers. The CPA should be set up at lowest possible cost in such a way as which it effectively and reliably delivers the functions required of it. It is intended that the policy would place UK PRS technology manufacturers in the best possible position to participate in the emerging market for that technology and would ensure that potential PRS users have reliable and secure access to PRS signal.

What policy options have been considered, including any alternatives to regulation? Please justify preferred option (further details in Evidence Base)
 Option 1: Do nothing
 Option 2: New government body – CPA is established as a new entity. All functions carried out in-house.
 Option 3: De minimus approach – CPA functions are outsourced to the CPA of another Member State in as much as those functions do not conflict with national sovereignty.
 Option 4: Federated approach – All CPA functions are outsourced to leverage existing capabilities across other parts of government.
 Option 5: (Preferred option): Amalgamated approach – Key CPA function are held within part of the UK Space Agency while the most security sensitive or less intensive elements are outsourced to Other Government Departments (OGDs).

Will the policy be reviewed? It will not be reviewed. **If applicable, set review date:** Month/Year

Does implementation go beyond minimum EU requirements?			No		
Are any of these organisations in scope? If Micros not exempted set out reason in Evidence Base.	Micro No	< 20 Yes	Small Yes	Medium Yes	Large Yes
What is the CO ₂ equivalent change in greenhouse gas emissions? (Million tonnes CO ₂ equivalent)			Traded: 0	Non-traded: 0	

I have read the Impact Assessment and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the leading options.

Signed by the responsible
 SELECT SIGNATORY:

..... Mark Franks Date: 13/06/2012

Summary: Analysis & Evidence

Policy Option 2

Description: New government body - a Competent PRS Authority is established as a new entity with all the resource for undertaking every function of the CPA held in house.

FULL ECONOMIC ASSESSMENT

Price Base Year	PV Base Year	Time Period Years	Net Benefit (Present Value (PV)) (£m)		
			Low: -4.091m	High: -13.026m	Best Estimate: -7.236m
2012	2012	10			
COSTS (£m)		Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)	
Low	£0.55m	1	£0.421m	£4.091m	
High	£3m		£1.186m	£13.026m	
Best Estimate	£1.775m		£0.646m	£7.236m	
Description and scale of key monetised costs by 'main affected groups'					
Exchequer: Key transition costs (£1.775m) are the purchase of the point of contact platform (POC-P) and building of secure infrastructure to accommodate POC-P. Ongoing costs (£0.646m per annum) correspond to the staffing, accommodation and capabilities costs of monitoring and managing PRS technology users and manufacturers in-house by the UK CPA.					
Other key non-monetised costs by 'main affected groups'					
BENEFITS (£m)		Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)	
Low	Optional		Optional	Optional	
High	Optional		Optional	Optional	
Best Estimate	n/k		n/k	n/k	
Description and scale of key monetised benefits by 'main affected groups'					
N/a					
Other key non-monetised benefits by 'main affected groups'					
PRS technology users: PRS offers benefits to potential PRS users (who may include emergency services and critical national infrastructure) such as resilience to spoofing (the production of false satellite navigation signals, convincing a receiver it is in the wrong place/time) and availability in times of crisis. PRS technology manufacturers: Access to the (as yet unquantified) market for PRS which without the set-up of a CPA is denied.					
Key assumptions/sensitivities/risks			Discount rate (%)	3.5	

BUSINESS ASSESSMENT (Option 1)

Direct impact on business (Equivalent Annual) £m:			In scope of	Measure qualifies
Costs: 0	Benefits: n/k	Net: n/k	No	NA

Summary: Analysis & Evidence

Policy Option 3

Description: De minimus option - a Competent PRS Authority is established which outsources all CPA functions to the CPA of another Member State in as much as those functions do not conflict with national sovereignty.

FULL ECONOMIC ASSESSMENT

Price Base Year 2012	PV Base Year 2012	Time Period Years 10	Net Benefit (Present Value (PV)) (£m)		
			Low: -3.225m	High: -7.442m	Best Estimate: -5.333m

COSTS (£m)	Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	£0m	£0.382m	£3.225m
High	£0m	£0.880m	£7.442m
Best Estimate	£0m	£0.631m	£5.333m

Description and scale of key monetised costs by 'main affected groups'

Transition costs are nil as existing infrastructure in another Member State (MS) is used in this Option. Ongoing costs (£0.631m per annum) correspond to the costs of outsourcing the hosting of the POC-P and maintaining a permanent connection to the Galileo Security Monitoring Centre (GSMC) in another MS, as well as employing another MS's capability in technology manufacturer and user oversight. Functions such as export control and crypto distribution are still held within a UK CPA, however.

Other key non-monetised costs by 'main affected groups'

BENEFITS (£m)	Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low	n/k	n/k	n/k
High	n/k	n/k	n/k
Best Estimate	n/k	n/k	n/k

Description and scale of key monetised benefits by 'main affected groups'

Other key non-monetised benefits by 'main affected groups'

PRS technology users: PRS offers benefits to potential PRS users (who may include emergency services and critical national infrastructure) such as resilience to spoofing and availability in times of crisis. PRS technology manufacturers: Access to the market for PRS which is not possible without the UK designating a CPA. The potential gains for entry into the market for PRS could be reduced, however, if use of the CPA of another MS leads to commercial risks.

Key assumptions/sensitivities/risks

Discount rate (%) 3.5

In the absence of existing CPAs in other MSs the estimates of the cost of contracting certain CPA functions from another MS were calculated using cost estimates of those of those functions which would incur a marginal cost to the other MS CPA. It is assumed a "consultancy premium" in the range of 0-50% (best estimate 25%) would be charged over the costs of service delivery to recover some of their investment costs, for example in the Point of Contact Platform.

BUSINESS ASSESSMENT (Option 2)

Direct impact on business (Equivalent Annual) £m:	In scope of	Measure qualifies
Costs: 0	No	NA
Benefits: n/k		
Net: n/k		

Summary: Analysis & Evidence

Policy Option 4

Description: Federated Approach - the role of the Competent PRS Authority is held within part of an existing UK government entity which simply acts as co-ordinator. All functions are outsourced to leverage existing capability in OGDs.

FULL ECONOMIC ASSESSMENT

Price Base Year 2012	PV Base Year 2012	Time Period Years 10	Net Benefit (Present Value (PV)) (£m)		
			Low: -£2.176m	High: -£10.592m	Best Estimate: £5.052m
COSTS (£m)					
		Total Transition (Constant Price) Years		Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low		£0.05m	1	£0.251m	£2.176m
High		£2m		£1.016m	£10.592m
Best Estimate		£1.025m		£0.476m	£5.052m
<p>Description and scale of key monetised costs by 'main affected groups'</p> <p>Exchequer: Key transition costs (£1.025m) are the purchase of the point of contact platform (POC-P). Ongoing costs (£0.476m per annum) correspond to leveraging the staffing, accommodation and technological capability costs of monitoring and managing PRS technology users and manufacturers from existing capabilities across other government departments (OGDs).</p>					
<p>Other key non-monetised costs by 'main affected groups'</p>					
BENEFITS (£m)					
		Total Transition (Constant Price) Years		Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low		n/k		n/k	n/k
High		n/k		n/k	n/k
Best Estimate		n/k		n/k	n/k
<p>Description and scale of key monetised benefits by 'main affected groups'</p>					
<p>Other key non-monetised benefits by 'main affected groups'</p> <p>PRS technology users: PRS offers benefits to potential PRS users (who may include emergency services and critical national infrastructure) such as resilience to spoofing and availability in times of crisis. The benefits to the users could be reduced under this option if poor coordination between the providers of CPA functions results in a poorer service to users. PRS technology manufacturers: Access to the market for PRS which is not possible without the UK designating a CPA.</p>					
<p>Key assumptions/sensitivities/risks</p> <p>Assumption of full commitment from OGDs. Use of OGD capability, especially in a time of fiscal austerity, could result in CPA functions being increasingly dropped in favour of internal priorities.</p>					<p>Discount rate (%)</p> <p>3.5</p>

BUSINESS ASSESSMENT (Option 3)

Direct impact on business (Equivalent Annual) £m:			In scope of	Measure qualifies
Costs: 0	Benefits: n/k	Net: n/k	No	NA

Summary: Analysis & Evidence

Policy Option 5

Description: Amalgamated approach - a CPA is set up within part of an existing government entity to undertake key CPA functions whilst outsourcing the most security sensitive or less intensive elements to OGDs.

FULL ECONOMIC ASSESSMENT

Price Base Year 2012	PV Base Year 2012	Time Period Years: 10	Net Benefit (Present Value (PV)) (£m)		
			Low: -3.412m	High: -£6.883m	Best Estimate: -£5.148m
COSTS (£m)		Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant	Total Cost (Present Value)	
Low	£0.05m	1	£0.263m	£2.271m	
High	£2m		£1.174m	£11.920m	
Best Estimate	£1.025m		£0.488m	£5.148m	
<p>Description and scale of key monetised costs by 'main affected groups'</p> <p>Exchequer: The key transition cost (£1.025m) is the purchase of the point of contact platform (POC-P). Ongoing costs (£0.488m per annum) correspond to costs incurred leveraging the most security sensitive CPA functions (hosting of secure infrastructure) from existing capability in OGDs while carrying out the more labour-intensive functions in-house.</p>					
<p>Other key non-monetised costs by 'main affected groups'</p>					
BENEFITS (£m)		Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant	Total Benefit (Present Value)	
Low	n/k		n/k	n/k	
High	n/k		n/k	n/k	
Best Estimate	n/k		n/k	n/k	
<p>Description and scale of key monetised benefits by 'main affected groups'</p>					
<p>Other key non-monetised benefits by 'main affected groups'</p> <p>PRS technology users: PRS offers benefits to potential PRS users (who may include emergency services and critical national infrastructure) such as resilience to spoofing and availability in times of crisis.</p> <p>PRS technology manufacturers: Access to the (as yet unquantified) market for PRS which is not possible without the UK designating a CPA.</p>					
Key assumptions/sensitivities/risks				Discount rate (%)	3.5
<p>Assumption of full commitment from OGDs. Use of OGD capability, especially in a time of fiscal austerity, could result in CPA functions being increasingly dropped in favour of internal priorities. This risk is reduced under this Option as the more labour-intensive functions are carried out in-house.</p>					

BUSINESS ASSESSMENT (Option 4)

Direct impact on business (Equivalent Annual) £m:			In scope of	Measure qualifies
Costs: 0	Benefits: n/k	Net: n/k	No	NA

Evidence Base (for summary sheets)

Problem under consideration

Public Regulated Service (PRS)

1. Galileo is a satellite navigation system currently being built by the European Union (EU) in collaboration with the European Space Agency (ESA). A key objective underpinning the rationale for building Galileo is to give EU Member States independence from satellite navigation systems operated by other countries. The most mature of these systems is still the US GPS system. Although unlikely, this could technically become unavailable in times of crisis or conflict (along with the Russian Glonass and Chinese Compass systems). Galileo differs from other satellite navigation systems in that it is conceived as a civil system under civil control, unlike others whose primary function is military.
2. One of the services which Galileo offers is a “public regulated service” (PRS). The PRS signal will be restricted to government-authorized users, and used for sensitive applications which require a high level of service continuity. Other Galileo services include an Open Signal, available without charge for use by anyone with appropriate mass-market equipment, a Commercial Service which will be chargeable to users and a Search & Rescue Service which adds functionality to existing satellite based Search & Rescue Capability.
3. Once PRS becomes available there are a number of users for whom it would potentially be useful. These include emergency services and critical national infrastructure. The key advantage offered by PRS over conventional free to air “open” services is better resilience due to the highly encrypted, authenticated signal. This offers some protection against spoofing¹, and would allow PRS users to continue to operate in the event that the Open Signal were unavailable.

Competent PRS Authority

4. The way in which Member States (MSs) access PRS is set out in Decision No 1104/2011/EU² and is the subject of this Impact Assessment. This Decision states that any MS wishing to use the PRS will need to designate a “Competent PRS Authority” (CPA) which will manage and monitor the manufacture, ownership and use of PRS receivers by natural persons living on the territory of that Member State and legal persons established on the territory of the Member State. According to the Decision, this CPA must be designated before 6 November 2013, i.e. within two years of the Decision’s publication.
5. This Impact Assessment and the related Consultation seeks to address whether the UK should set up a Competent PRS Authority in order for users to gain authorisation and access to the PRS signal and for manufacturers to develop and build PRS technology and if so, what form the CPA should take.

¹ With spoofing, an adversary provides fake satellite navigation signals. This convinces the signal receiver that it is located in the wrong place and/or time.

² Decision No 1104/2011/EU of the European Parliament and of the Council of 25 October 2011 on the rules for access to the public regulated service provided by the global navigation satellite system established under the Galileo programme.
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:287:0001:0008:EN:PDF>

Background

6. The functions legally required of a Competent PRS Authority are detailed in full in Articles 5(4) and 5(5) of Decision 1104/2011/EU, as outlined in Annex 1.

7. A CPA has a wide breadth of responsibility, some pertaining to the authorisation and monitoring of PRS users and some pertaining to authorisation and monitoring of the manufacturers of PRS technology.

8. In order to build a clear picture of what the functions of a CPA entail and to provide background on what the costs of serving those functions might be, the practicalities surrounding the use and manufacture of PRS technology are detailed below.

PRS technology users

Potential PRS technology users

9. PRS access is restricted to government-authorized users for sensitive applications which require effective access control and a high level of service continuity. The scope of what type of users can be granted access to PRS may be decided by Member States as Article 3(3) of Decision 1104/2011 states that “*each Member State which uses PRS shall decide independently which categories of natural persons residing on its territory or performing official duties abroad on behalf of that Member State and legal persons established on its territory are authorised to be PRS users, as well as the uses to which PRS may be put*”.

10. A PRS Application Concept Involving Future Interested Customers (PACIFIC³) project involving 20 companies from more than 14 European countries was carried out in 2007/8 to scope the potential user base of PRS. PACIFIC identified and surveyed 200 user communities across the EU and Norway in several application areas. This study provided an initial insight to potential PRS user communities but would likely benefit from further development, not least to update it in line with current thinking.

11. The possible applications noted across MSs could include:

- **Law enforcement** (Police, Special Ops, Customs).
- **Emergency Services** (Fire brigades, ambulances, civil protection)
- **Defence** (Army, Marine, Air Force)
- **Critical Telecom** (Network operators)
- **Critical Energy** (Energy suppliers)
- **Critical Transport** (Civil aviation)
- **Strategic Activities** (Commercial ports, space agencies)

Selection of authorised PRS users in the UK

12. The wider the umbrella of users is spread, the larger the potential uptake of PRS. This would enable more users to benefit from the service, accelerate the proliferation of PRS technology and help to reduce the equipment unit cost. Insofar as the UK has a competitive

³ <http://gsa.europa.eu/projects/pacific/www.prs-pacific.eu/index.html>

advantage in developing PRS technology, a wider user base could well benefit UK manufacturing, as well as demonstrating the range of PRS applications to other MSs.

13. Equally, the risk of PRS receivers being lost increases as the user base expands and poses a threat to the security of the service. Additionally, if the technology is intended to increase Government resilience in times of crisis, then Government may prefer to be more selective in the way that it designates government authorised users.

14. Early consultation with stakeholders (PRS technology manufacturers and potential users) indicates that the potential PRS user community should be defined in a way so as to best place UK PRS manufacturers in the emerging market for PRS technology, while ensuring the security of the service. The UK military has indicated that its needs are fully met by GPS and thus has no current need for PRS.

15. Current UKSA thinking is that PRS use could be authorised to UK critical national infrastructure, namely the facilities, systems, sites and networks necessary for the delivery of the essential services upon which daily life in the UK depends. Where this introduces ambiguity, access might be granted to a user based on whether a function is undertaken for largely for commercial gain or whether an attack against a function of the user might be considered an attack against the State. The PRS user community will be further scoped during consultation.

How is PRS access granted?

16. The Competent PRS Authority is responsible for processing requests for PRS access from potential users. A Competent PRS Authority is the interface between national user communities and the wider Galileo security infrastructure.

17. At the heart of the CPA is a classified server which manages the encrypted keys for all PRS receivers under UK control, the Point of Contact Platform (POC-P). This is the main set-up cost associated with establishing a CPA. Significant running costs apply, as does the cost of maintaining a permanent communication link between the Galileo Security Monitoring Centre (GSMC) and the CPA. These are discussed in more detail in the Costs section below. Once the CPA becomes operational, government-authorised users would be able to obtain PRS receivers and technology which, along with their user keys, allow them to read the PRS signal.

What is meant by PRS access rights?

18. PRS access rights define the way in which a user or user group intends to use PRS satellite navigation services.

19. Any position obtained by satellite navigation is derived by receiving very precise timing signals from a number satellites and using that data to calculate a position. This means that satellite navigation can provide

- Accurate Positioning or location data
- Accurate Navigation data (by drawing a line through a number of past positions to calculate speed and distance as well as a current position)
- Accurate Timing data to a scale of nanoseconds

20. This combination of Position, Navigation and Timing (PNT) means that PRS access is likely to be governed by the diverse needs of a range of user communities. Consequently, some users may be granted access rights to simply use the timing information (for time stamping purposes) whilst others may require access to positioning or navigation data. Some user communities may want to use the decrypted data remotely (e.g. to track assets from a central control room). Others may need the data presented directly on visual displays attached to the receivers themselves (as would be the case for a conventional satellite navigation unit). It is the responsibility of the CPA to define user access rights and to group users according to access rights.

Do users pay for PRS access rights?

21. A CPA will provide an interface between the user community and the wider Galileo security infrastructure. This means it will obtain encryption keys from the system and distribute them to authorised users. The question of whether users should be charged for this service requires careful consideration.

22. Each request to the Competent PRS Authority will incur a cost to the CPA and if the marginal benefit to the user is greater than this cost then objectively the PRS user should bear at least some of the cost of that transaction.

23. Early informal consultation with potential PRS users indicates that charging for PRS access would however severely limit PRS uptake, particularly in the early stages. Access to Open Service alternatives from either GPS or Galileo is free. Thus a charge for PRS use is likely to deter initial user uptake. It should also be considered, that PRS is an embryonic technology, the benefits of which are subject to high uncertainty and may lower the perceived value that potential users place on access to the service.

24. If the UK wishes to accelerate the proliferation of PRS technology, then charging for access at the outset is not advised. There are two main arguments why the UK should wish to encourage early uptake of PRS. Firstly, the UK has made a strong commitment to the European Commission's Galileo programme through its wider contribution to the EU budget. To capitalise on investment in Galileo to date, PRS should be supported in its early stages of development. Secondly, UK industry has had a key involvement with the early stages of PRS technology development. The UK's high tech manufacturing capability and the strength of its space industry means that it has been highly successful in competing for key contracts that have been funded under the programme. It is poised to play a potentially pivotal role in a nascent market which has the potential to be extremely lucrative.

25. As PRS use becomes more widespread and its benefits become apparent, the potential for charging users for certain services could be considered. Ideally, this could help to ensure that the CPA could, in time, be operated on a cost neutral basis. The consultation will seek to gather information on what the effects of charging users for PRS access would be.

PRS technology manufacturers

Restrictions on the manufacture of PRS technology

26. 'PRS technology' refers to PRS receivers and security modules. PRS technology manufacture is only permitted in a Member State which has designated a Competent PRS Authority. Paragraph 17 of Decision 1104/2011/EU states that "*with regard to receiver manufacturing and security, security requirements make it necessary for this task to be entrusted only to a Member State which has designated a competent PRS authority or to undertakings established on the territory of a Member State which has designated a competent PRS authority*". Thus, a CPA would have to be set up in the UK if UK manufacturers wished to participate in the market for PRS technology.

27. In addition, receiver manufacturers must be fully authorised by the Security Accreditation Board for European Global Navigation Satellite Systems (GNSS) and must comply with its decisions. CPAs will continuously monitor compliance both with that authorisation requirement and those decisions. A CPA also monitors compliance with specific technical requirements stemming from the common minimum standards (the extract from the Decision's Annex outlining the areas these will cover are listed in Annex 2).

28. A manufacturer who is authorised to manufacture PRS technology in the UK may export the technology to other MSs without restrictions. Should they wish to manufacture equipment for export outside the EU, export controls apply, as outlined in Decision 1104/2011/EU.

Market outlook for PRS technology

29. The market for PRS depends on how the user community for PRS develops. As mentioned previously, PRS is an embryonic technology and questions remain surrounding the uptake of the service and the value it will be perceived to add for its eventual user community. The first PRS signals became available in 2010 for validation and testing in a simulated environment. Following the successful launch of the first two in-orbit validation (IOV) satellites in October 2011, PRS signals from orbiting satellites are now being received by number of test receivers. The European Commission envisages PRS will not become fully operational before 2018.

30. Key factors that are likely to significantly influence how PRS is used and by whom, will include the "retail" price of receivers, the administrative overhead for user groups, any other obligations imposed on user communities through the common minimum standards (as outlined in Annex 2), how MSs manage access at national level through their CPAs and whether any charges are applied by MSs for either access to or usage of the service. The UK Space Agency recently issued a call to pilot end-to-end PRS capability with a particular emphasis on the management of encryption keys. Ultimately, the principle output of this work will be to develop applications which directly add value to end user communities. This should provide stronger insights to the breadth of the future PRS user base, both in the UK and elsewhere in Europe.

31. A market study for Global Navigation Satellite Systems (GNSS) is being conducted by the European GNSS Agency, (GSA; formerly European GNSS Authority). It is being conducted in two parts: top-down market research which will provide preliminary assumptions of what the market positioning of PRS within the market for GNSS will be and bottom-up market research which will use in-depth interviews with key stakeholders in order to validate the assumptions made in the top-down report and to refine the market quantification and PRS market share. It is envisaged that the findings of these reports will

become available while the consultation on the CPA is ongoing and will help to provide a picture of the size of the market which PRS technology manufacturers can enter.

32. The European Commission has drawn analogies to the value of the military GPS market which would estimate the potential value of the PRS market at €7bn as the constellation builds up and the user base increases. It is believed that the military GPS market in Europe is nowhere near this figure and, whilst PRS is potentially a dual use technology, its primary use is intended in a civilian context. This figure is therefore not used to estimate the value of the market for the UK.

Rationale

33. The government should intervene due to regulatory failure. Decision 1104/2011/EU states that a Competent PRS Authority, authorising and monitoring the use and manufacture of PRS technology, must be created in order for a UK user to access PRS, or for UK manufacturers make PRS technology. Under current UK legislation (or lack of it), UK firms would not be able to benefit from commercial opportunities in this area and potential PRS users in the UK, who could include critical national infrastructure and emergency services, cannot derive benefit from the use of PRS.

34. The PRS is a service to which the general public will not have access. Its use will require oversight to ensure security is maintained. Moreover, certain applications of the service may be sensitive and the system itself comprises classified and protected technologies which must be controlled to prevent proliferation to unlicensed users which could undermine the system through misuse and abuse. It is therefore necessary to ensure users comply with clear standards which establish an authorisation procedure via the CPA and safeguard the use and storage of encryption keys, receivers and any other PRS related technology.

Policy objectives

To create the authorisation capability for PRS use in the UK

- Government entities, organisations acting in lieu of government and critical national infrastructure have access to a resilient, authenticated GNSS signal even in times of crisis.

To create the authorisation capability for PRS technology manufacture in the UK

- UK manufacturers who have the technological capability and security clearance to manufacture PRS technology are able to access the market for PRS technology at an early stage.

To create a monitoring and enforcement capability to ensure compliance with the common minimum standards among PRS users and PRS technology manufacturers

- The use and manufacture of PRS technology does not compromise the security or the integrity of the service.
- The penalty system applicable when the common minimum standards are infringed is effective, proportionate and dissuasive.

Options considered

35. If a CPA is set up, the question remains what form that body should take. Member States wishing to set up a CPA have autonomy in deciding its form. Five options, including a Do Nothing option, have been identified:

Option 1: Do nothing

36. Under this Option, no Competent PRS Authority is set up. The UK does not designate a CPA in another Member State to undertake CPA activities. UK manufacturers are unable to manufacture PRS receivers and there can be no deployment of PRS technology to UK user communities.

37. A point of contact to assist in reporting detected potentially harmful electromagnetic interference⁴ affecting PRS must in any case be designated. This function is currently being undertaken from within the UK Space Agency.

Option 2: New government body

38. A Competent PRS Authority is established as a new entity with all the resource for undertaking every function of the CPA held in-house. In other words, all 9 CPA functions identified in Annex 1 are performed by this new entity.

39. The new entity must be within government as the responsibilities of “Competent Authorities” rest directly with Member States”. This rules out the creation of a Non Departmental Public Body, which is in line with Coalition priorities. According to Cabinet Office guidance, a new public body carrying out these functions would likely be a government office⁵.

Option 3: De minimus approach

40. Under this Option, a Competent PRS Authority is set up which outsources all CPA functions to the CPA of another Member State in as much as those functions do not conflict with national sovereignty.

41. The table in Annex 3 addresses each of the functions of the CPA in turn and considers how they may impact on UK sovereignty or other national interests if these functions were to be delegated to the CPA of another Member State.

42. Where there is a conflict with national sovereignty, these functions could be fulfilled by a de minimus UK CPA which could either be set up as an independent entity or accommodated within an existing Government entity. Further opinion on which of the CPA’s functions could be outsourced to the CPA of another MS will be sought through consultation.

⁴ Detection of potentially harmful electromagnetic interference refers to detection of jamming or spoofing devices.

⁵ http://www.civilservice.gov.uk/wp-content/uploads/2011/09/overview_tcm6-2489.pdf

43. A suggested ownership of CPA functions (either UK CPA or other Member State CPA) under the de minimus option is given in Table 1 on the basis of the arguments and recommendations in Annex 3.

Option 4: Federated approach

44. Under this option, the role of the Competent PRS Authority is held within part of an existing UK government entity which simply acts as co-ordinator to all the functions of the CPA which would be outsourced to leverage existing capabilities across other parts of government. The intention of this approach would be to deliver a comprehensive service at lowest possible cost.

45. An indication of what outsourced ownership could look like is outlined in Table 1. The intention is to identify the best possible partners through consultation and to assess their willingness to provide long term support to the role of the CPA.

Option 5: Amalgamated approach (preferred option)

46. This option is an amalgamation of Options 2 and 4. It retains “command and control” capability and key functions within part of an existing government entity whilst outsourcing the most security sensitive or less intensive elements to Other Government Departments (OGDs).

47. Table 1 below outlines the ownership of CPA functions under this Amalgamated approach. RF monitoring would sit with OFCOM and the classified infrastructure could be hosted where there is pre-existing capability to do so. Other more intensive and time-consuming functions such as accreditation and enforcement could be undertaken centrally to ensure greater reliability and access to designated resource.

Table 1. Overview of CPA function ownership by Options 1 - 5

CPA function (as in Articles 5(4) and 5(5) of Decision 1104/2011/EU)	Ownership of CPA function				
	Option 1: Do Nothing	Option 2: New government body	Option 3: De minimus approach	Option 4: Federated Approach	Option 5: (Preferred Option) Amalgamated approach
1. Ensure compliance with the common minimum standards	n/a	UK CPA	UK CPA	UKSA/DfT/MoD	UK CPA
2. Grouping of users for the management of the PRS with the Galileo Security Monitoring Centre (GSMC)	n/a	UK CPA	UK CPA	UKSA / Home Office / MoD	UK CPA
3. Determine and manage the PRS access rights for each group or user	n/a	UK CPA	UK CPA	UKSA / Home Office / MoD	UK CPA
4. Obtain the PRS keys and other related classified information from the GSMC	n/a	UK CPA	Other MS CPA	GCHQ / NSA / MoD	UK CPA / GCHQ / NSA / MoD
5. Distribute PRS keys and other related classified information are distributed to users	n/a	UK CPA	UK CPA	GCHQ / NSA / MoD	UK CPA / GCHQ / NSA
6. Manage the security of the receivers and associated classified technology and information and assess the risks	n/a	UK CPA	UK CPA	UKSA / Home Office / GCHQ / NSA / MoD	UK CPA
7. Establish a point of contact for assisting as necessary in the reporting of detected potentially harmful electromagnetic interference affecting the PRS	OfCom / UKSA	UK CPA	UK CPA	OfCom	Point of Contact: UK CPA; RF detection capability - OfCom
8. Ensure that a body established on the territory of its Member State may only develop or manufacture PRS receivers or modules if such a body (a) has been duly authorised by the Security Accreditation Board in accordance with Article 11 (2) of Regulation (EU) No 912/2010; and (b) complies both with the decisions of the Security Accreditation Board and with Article 8 and point 2 of the Annex regarding the development and manufacture of PRS receivers or security modules, in so far as these relate to its activity.	n/a	UK CPA	Other MS CPA	UKSA / CPNI / BIS / MoD / DfT	UK CPA
9. In the case of export outside the Union, act as an interface to the entities competent for export restrictions of relevant equipment, technology and software regarding the use, development and manufacturing of the PRS.	n/a	UK CPA	UK CPA	UKTI DSO Exports	UKTI DSO Exports / GCHQ

Detailed Costs and Benefits

Level of evidence collected

48. All the evidence required to accurately quantify the costs and benefits of the various options for the form of the Competent PRS Authority is difficult to fully gather at this stage given the embryonic nature of PRS technology. Were PRS technology already fully developed this would aid in giving an accurate indication of the costs of capability required (both in terms of staff and technical equipment) to deliver CPA functions. Similarly, some of the benefits to PRS users will only be revealed once the technology is up and running. Most importantly, the EC is still developing the common minimum standards (CMS) for Security which underpin PRS management and manufacture. Unfortunately the EC is not expected to finalise the CMS until late 2014. This leaves no time for MSs to take them fully into account when considering the structures they need to develop their CPAs which need to be set up within 2 years of the Decision's publication, 4 November 2011.

49. The UK is taking a leading position in implementing Decision 1104/2011/EU to ensure it is well equipped to capitalise on the commercial opportunities offered by PRS. Thus, a similar policy implementation has not yet occurred in any other Member States from which this appraisal could draw evidence.

50. In estimating costs and benefits at this stage an amount of informal consultation has occurred with Other Government Departments, PRS industry stakeholders, PRS experts and the European GNSS Agency. Where preliminary consultation has occurred this is highlighted clearly below.

51. Further evidence gathering was not deemed proportionate at this point due to uncertainty surrounding what the PRS system will look like. An informed comparison can be made between options with the evidence gathered as the *relative* cost of options becomes apparent. Some estimates are rough by necessity but have been made at this point to allow inter-option comparison. Further evidence is sought in the consultation stage in addition to the evidence which will be made available as PRS studies (such as the UKSA PRS pilot and the GSA PRS market study) are completed.

Identifying winners and losers

52. The key stakeholders in this instance include the potential manufacturers of PRS technology and the potential users of PRS technology in the UK. The form that the CPA takes will largely impact on these two groups.

Effect on small businesses

53. Manufacturers of PRS equipment may need to undergo a site facility clearance process to enable them to hold classified materials on site. The cost associated with obtaining this status will vary from site but may be relatively high. UK Government is considering how this impact could be mitigated, including, the possibility of designating a central facility that SMEs and other organisations could use as a way of being able to access the necessary information – subject to holding the appropriate level of personnel security clearances.

54. This is an indirect cost, however, as the proposed legislation would not obligate any businesses to undertake this site facility clearance process. It would only be undertaken by those businesses which choose to manufacture PRS technology.

Costs

Transition Costs

55. The key transition costs in forming the CPA are identified in Table 2 below, along with evidence sources and key assumptions made. The price base year for these estimates is 2012. These costs would be borne within the first year of the establishment of the CPA. It is considered likely that most of these costs may need to be borne within Government.

Recurring costs

56. The recurring costs associated with the different options for a CPA are outlined in Table 3 below along with evidence sources and key assumptions made. The price base year for these estimates is 2012. These costs would be borne following the first year of the establishment of the CPA. It is envisaged that these costs may initially need to be borne by the CPA. As the market for PRS develops, the user community expands and the benefits of PRS become clearer, the possibility is not ruled out that the CPA would begin to charge for its services and seek to operate on a cost neutral basis. The possibility also exists that a UK CPA would sell its services to smaller MSs who may wish to access PRS without incurring the costs of setting up a CPA of their own.

Table 2. Transition costs for Options 1 – 5

	Option 1: Do nothing	Option 2: New government body	Option 3: De minimus	Option 4: Federated approach	Option 5 (Preferred Option): Amalgamated approach	Notes/assumptions
Point of contact platform (POC-P)	0	£1,025,000	0	£1,025,000	£1,025,000	<p>A POC-P is the main set-up cost associated with the CPA. It is a classified server which is a secure platform that will enable PRS access management. A POC-P is required in options 2, 4 and 5 as the ownership of PRS access management is held in-house under these options.</p> <p>POC-P technology remains in its developmental phase and the UK is considering a range of technologies which estimates the cost of a POC-P anywhere between £50k for a minimal platform to £2m for a fully operational system. The range is defined by the technologies employed, the level of protection required by the Common Minimum Standards that are currently being developed in Europe and the complexity of the interface between the CPA and the wider Galileo infrastructure. Due to the high level of uncertainty surrounding this technology, the mid-point in this range, £1,025,000 is taken as the best estimate.</p> <p>As these technologies develop, all options will be kept under review. The UKSA is also undertaking pilot work that hopes to see significant reductions in key management overhead as one of its outputs. It is hoped that this will also help to reduce the cost of building and purchasing a POC-P. Early findings from this pilot study will become available during consultation.</p> <p><i>Source: Estimates from industry sources and independent technical advice.</i></p>

Building secure infrastructure (POC-P)	0	£750,000	0	0	0	<p>The POC-P contains technology classified to Secret. The secure infrastructure is necessary to provide an appropriately protected operating environment which meets this standard.</p> <p>Under Option 2 this secure infrastructure would be based in-house by a UK CPA. Building the secure infrastructure would cost £500k - £1m, with a best estimate of £750k.</p> <p>Under Options 3, 4 and 5 existing secure facilities would be used and as such no transition cost would be incurred.</p> <p><i>Source: Estimate from Defence Science and Technology Laboratory (DSTL) and industry sources</i></p>
Total Transition Costs	0	£1,775,000	0	£1,025,000	£1,025,000	

Table 3. Recurring costs for Options 1 - 5

	Option 1: Do nothing	Option 2: New government body	Option 3: De minimus	Option 4: Federated approach	Option 5 (Preferred Option): Amalgamated approach	Notes/assumptions
Accommodation costs of new CPA body	0	£19,000	0	£5,500	£18,000	The basis of these calculations is in Annex 4, where staff and location requirements for the UK CPA under each option are outlined. <i>Source: BIS Infrastructure Services Estimate</i>
Staff capability to manage users: determining access rights, key distribution, cryptography	0	£20,557	£25,696	£20,557	£20,557	These functions are completed in-house in the UK CPA under Options 2 and 5. Under Option 4 these functions are completed in Other Government Departments. These tasks require the same labour input under each option. Cost calculated as 0.5 FTE [<i>Source: UKSA calculation</i>] where $\text{FTE} = [\text{SEO wage}^6 + 16.4\% \text{ non-wage labour costs}^7]$ $= £35,321 * 1.164$ $= £41,114$ $0.5 \text{ FTE} = £41,114 * 0.5$ $= £20,557$ Under Option 3 this function is carried out by a CPA in another Member State (MS). It is assumed that another MS would require more resource than a UK CPA to carry out this function as it would be performing UK user management from abroad and thus be subject to logistical and distance barriers. Indicative estimates of this premium range from 0 to 50% [<i>Source: UKSA estimate</i>].

⁶ SEO wage calculated as SEO target rate from BIS pay offer for 1 Aug 2011 to 31 July 2012.

⁷ Latest Eurostat figures for Social security and other labour costs paid by employer 14.1% as a percentage of total labour costs. The relevant multiplier of wage costs to reflect non-wage costs is 16.4%. (1/85.9). http://epp.eurostat.ec.europa.eu/portal/page/portal/labour_market/labour_costs/main_tables

						<p>£20,557 * 1 = £20,557 £20,557 * 1.5 = £30,836 The mid-point of this range (25%) is taken as a best estimate £20,557 * 1.25 = £25,696</p> <p><i>Source: UKSA estimates</i></p>
Hosting of secure infrastructure (POC-P)	0	£200,000	£112,500	£25,000	£25,000	<p>The POC-P contains technology classified to Secret. The secure infrastructure is necessary to provide an appropriately protected operating environment which meets this standard.</p> <p>Under Option 2 this function would be carried out in-house by a UK CPA. It is estimated that the cost of renting and operating the space for a hermetically sealed box in the purpose-built guarded site would cost £200,000 per annum.</p> <p>Under Options 4 and 5 the CPA would use pre-existing infrastructure at either the International Space Innovation Centre at Harwell or the DSTL site at Porton Down. These estimates of £25,000 per annum include the cost of renting the space in a guarded site to host the POC-P but also the costs associated with extracting heat from the hermetically sealed box.</p> <p>Under Option 3 this function would be outsourced to an alternative location in another member state. It is assumed that another MS would require more resource than a UK CPA to carry out this function for an outsourced service which provided the necessary infrastructure. As this is not a marginal cost incurred by the CPA of another MS a premium is not added to the cost as has been calculated for other costs above. It is assumed other MS CPA will charge a rent for the use of the POC-P at a level to recover their annual costs as well as a portion of their investment in a POC-P. It is assumed the lower bound of this rent is £25,000 and the upper bound £200,000. In the absence of further information at this stage the mid-point of these estimates,</p> <p><i>Source: Estimates from Defence Science and Technology Laboratory (DSTL) and industry sources</i></p>

Key management	0	£200,000	£200,000	£200,000	£200,000	<p>Key management services will involve distributing the encrypted keys to PRS users once they have been authorised by the CPA. This function will be held within HMG and initial consultation with the Communications Electronics Security Group implies that CESG will have some involvement in this function. The cost of this function has been estimated at £100k - £300k per annum, with a best estimate of £200k.</p> <p>This figure is the same under all options. It is not a CPA function that would be outsourced under Option 3.</p> <p><i>Source: Estimate from the Communications Electronics Security Group (CESG)</i></p>
Cost of establishing a permanent connection from CPA to GSMC	0	£16,000	£38,000	£16,000	£16,000	<p>Under Options 2, 4 and 5 a connection to the GSMC from the UK CPA needs to be established. The GSA envisages this connection being permanent.</p> <p>The cost of a typical dedicated 2 megabyte pipe depends on where the UK CPA is located. Both the International Space Innovation Centre at Harwell and the DSTL site at Porton Down are potential locations for the POC-P. The European Commission and the European Space Agency are considering how best to manage the connections between POC-Ps and Galileo infrastructure and the costs associated with providing that capability. A cloud connection is also possible, however. The best analogy to known costs within UK government is the cost of connecting to Government Secure Intranet (GSI) estimated at £16,000 per annum.</p> <p>Under Option 3 this function would be undertaken by another MS. GSA estimates that the function would cost £60,000. In the absence of lower estimates from another MS the mid-point between this estimate and the GSI estimate is taken as a best estimate.</p> <p>Best estimate = $(£16,000 + £60,000) / 2$ = £38,000</p> <p><i>Source: BIS IT Security Office</i></p>

Oversight of PRS technology manufacturers and users	0	£250,000	£312,500	£250,000	£250,000	<p>Under Options 2 and 5 manufacturer oversight sits within the UK CPA. Under Option 4 ownership of this function sits in OGDs (e.g. Cabinet Office, MoD, DfT). The recurring cost of this function is likely to be similar irrespective of where ownership of the function is based.</p> <p>Evidence from the GPS project office in MoD estimates that the cost is £700-750k to carry out similar functions to those required by the CPA. This is the cost of:</p> <ul style="list-style-type: none"> - Assuring compliance with the US obligations for military GPS that are imposed through NATO (technical security advice and security audits of both MoD projects and industrial partners/manufacturers) - Undertaking accreditation of equipment that is being developed. - Oversight of test facilities including jammers and GPS simulators (work which is subcontracted to DSTL). <p>This figure will not correspond exactly to the costs encountered by a UK CPA but has provided a starting point for early consultation. On the basis of this comparator, an indicative lower-bound estimate of £100k has been suggested (<i>Source: UKSA</i>) for these functions in relation to PRS, reflecting the fact that the number of PRS manufacturers is unlikely to approach double digits. An upper bound of £750k (<i>Source: MOD</i>) is taken, reflecting the current cost of this function for GPS. In the absence of further information at this point, a best estimate of £250k is taken to reflect the fact that a smaller number of manufacturers will operate in the market for PRS than they do for GPS, particularly at the outset of PRS technology development.</p> <p>Under Option 3 this function is carried out by a CPA in another Member State (MS). It is assumed that another MS would require more resource than a UK CPA to carry out this function as it would be performing UK technology oversight from abroad and thus be subject to distance and possibly language barriers. Indicative estimates of this premium range from 0 to 50%. £250,000 * 1 = £250,000</p>
---	---	----------	----------	----------	----------	---

						<p>£250,000 * 1.5 = £375,000 The mid-point of this range (25%) is taken as a best estimate £250,000 * 1.25 = £312,500</p> <p><i>Source: GPS Project Office, Ministry of Defence and UKSA calculations</i></p>
Staff capability for export control	0	£12,334	£12,334	£12,334	£12,334	<p>Under Options 2-5 ownership of these functions sits within the UK CPA, but also involves resource from GCHQ in signing off crypto export and from UKTI DSO Exports in overseeing UK exports.</p> <p>Cost calculated as 0.3 FTE [<i>Source: UKSA calculation</i>] where FTE = [SEO wage⁸ + 16.4% non-wage labour costs⁹] = £35,321 * 1.164 = £41,114</p> <p>0.3 FTE = £41,114 * 0.3 = £12,334</p> <p><i>Source: UKSA estimate</i></p>
Total recurring costs (per annum)	0	£717,891	£701,030	£529,391	£541,891	

⁸ SEO wage calculated as SEO target rate from BIS pay offer for 1 Aug 2011 to 31 July 2012.

⁹ Latest Eurostat figures for Social security and other labour costs paid by employer 14.1% as a percentage of total labour costs. The relevant multiplier of wage costs to reflect non-wage costs is 16.4%. (1/85.9). http://epp.eurostat.ec.europa.eu/portal/page/portal/labour_market/labour_costs/main_tables

Benefits

57. The benefits of Options 2 – 5 are assessed in comparison to the status quo ‘Do Nothing’ Option 1. A Competent PRS Authority unlocks the key benefits to the main parties affected, namely PRS technology users and manufacturers, regardless of the form the CPA takes. As such the benefits of Options 2 – 5 are treated together.

Benefits to potential PRS users

Option 1

58. Under the Do Nothing option, no potential PRS users are able to access PRS. Benefits will be assessed in relation to this option.

Options 2 – 5

59. The benefits to PRS users are in essence those benefits that PRS offers over other satellite navigation systems. The first Galileo satellites were launched in October 2011 and the first test of PRS signal receivers took place in March 2012. Thus, many of the benefits of PRS are only likely to be fully understood as the service and the technologies which support it become more mature.

60. The key benefits of PRS over other substitutes (such as Galileo Open Signal or GPS open signal) are likely to be:

- **Resilience to Spoofing.** Publicly available signal structures and interface control documentation make open GNSS services relatively easy to replicate spuriously. Existing GNSS infrastructures do not allow users to authenticate signals readily and in real-time, rendering them vulnerable to spoofing, the broadcast of fake GNSS-like signals, and meaconing (the rebroadcast of same GNSS signals to create confusion). PRS is highly encrypted which makes it far more resilient to spoofing. In this context, an additional benefit of PRS is that the complex nature of the encryption algorithm means that the signal identifies itself as authentic by virtue of being decrypted.
- **Resilience to Jamming.** Hostile or malicious GNSS jammers (devices which emit random noise to interfere with a signal) are proliferating, boosted by low prices and do-it-yourself information on GNSS. As critical infrastructure, GNSS is a likely target for malicious organisations. PRS signal broadcasts wideband signals on frequencies separate from GNSS open services, thus offering some resilience to jamming. In addition, technology can be built into receivers to help mitigate jamming, albeit at an extra cost.
- **Availability in times of crisis.** PRS is a highly encrypted service available only to government authorised users. In times of crisis or in the event that other GNSS signals may be temporarily unavailable, PRS services will continue to for those authorised to use it.
- **Interoperability with other GNSS services.** Although PRS is independent from other GNSS signals, it will be interoperable with GPS open services. In an increasingly multi GNSS environment, this sort of combined use is already being developed by receiver manufacturers to offer enhanced performance in terms of accuracy, integrity, continuity and availability of Position Navigation Timing (PNT) services, including greater resilience to interference and jamming.

Relative benefits to PRS technology users across options

61. Under Option 2, a new government body, PRS technology users are likely to enjoy the most comprehensive service from a CPA. Option 4, and possibly Options 3 or 5, carries the risk that the functions of the CPA might not be as well coordinated if they are sourced from different agencies and government departments.

62. Once PRS use has been authorised the benefits to PRS users are unlikely to vary very much across options, however. This is because the benefits of PRS outlined above derive from the technology, not from the CPA. The CPA is necessary to unlock these benefits, however.

Benefits to potential PRS technology manufacturers

Option 1

63. Under the Do Nothing option, no potential PRS users are able to access PRS and thus there are no benefits.

Options 2 - 5

64. The key benefits to PRS technology manufacturers of having a UK CPA will be the ability to access to the market for PRS.

65. Given that Member States are prohibited by Decision 1104/2011/EU from manufacturing PRS technology without the establishment of a Competent PRS Authority, the early establishment of a UK CPA could give UK firms a first mover advantage in the market for PRS technology. It is unclear currently how the market for PRS technology manufacture will look, but the European Commission envisages two core suppliers emerging. UK industry is already well placed to take advantage of the market, having had a strong involvement in the development of PRS technology to date and playing a key role in piloting PRS technology and applications.

66. A market study for PRS is being conducted by the European GNSS Agency, (GSA; formerly European GNSS Authority). The results of this study will become available to the UK during CPA Consultation and in providing an indication of the size of the market for PRS will give a better indication of the potential benefits to UK PRS technology manufacturers.

67. The European Commission has drawn analogies to the value of the military GPS market which would estimate the potential value of the PRS market at €7bn as the constellation builds up and the user base increases over the next ten years. This estimate has not been used for the purposes of estimating the scale of benefits as it was not deemed fit for the purpose of this Impact Assessment. It is believed that the military GPS market in Europe is nowhere near this figure and, whilst PRS is potentially a dual use technology, its primary use is intended in a civilian context.

Relative benefits to PRS technology manufacturers across options

68. As was the case for PRS users, so it is for PRS technology manufacturers that once PRS technology manufacture has been authorised the benefits to manufacturers in terms of access to the market for PRS should be largely the same across options 2 – 5.

69. Under Option 3, however, oversight of technology manufacturers lies with the CPA of another MS. This could hold significant commercial risks if that MS is a key competitor in the market for PRS. In that case the benefits under Option 3 could be less than under other options. It is assumed, however, that the CPA designated by the UK under Option 3 would be chosen to minimise this risk and any agreement signed would try to mitigate this risk.

Comparison of costs and benefits

70. As the benefits across Options 2 – 5 are largely similar, deriving from the existence of a CPA, the preferred option of Option 5 has been reached through a consideration of the costs associated with each option as well as some consideration of the risks associated with the different ways of delivering the CPA objectives. Table 4 below gives a summary of the transition and average annual costs of each option, along with the total cost in present value.

Table 4. Total transition and recurring costs for Options 1 – 5.

		Option 1: Do Nothing	Option 2: New government body	Option 3: De minimus	Option 4: Federated approach	Option 5: Amalgamated approach
Transition Costs	Low	£0m	£0.550m	£0m	£0.050m	£0.050m
	High	£0m	£3.000m	£0m	£2.000m	£2.000m
	Best estimate	£0m	£1.775m	£0m	£1.025m	£1.025m
Average Annual (Excluding transition, constant price)	Low	£0m	£0.421m	£0.382m	£0.251m	£0.263m
	High	£0m	£1.186m	£0.880m	£1.016m	£1.174m
	Best estimate	£0m	£0.646m	£0.631m	£0.476m	£0.488m
Total Cost (present value)	Low	£0m	£4.091m	£3.225m	£2.176m	£2.271m
	High	£0m	£13.026m	£7.442m	£10.592m	£11.920m
	Best estimate	£0m	£7.236m	£5.333m	£5.052m	£5.148m

71. Under Option 3, the de minimus option, transition costs are nil but annual recurring costs are higher than under any other option. The risks associated with this option are considerably higher than under other options, however, as PRS user management and monitoring is outsourced to the CPA of another country. This would expose PRS users, likely to be key parts of government or services on which government is critically reliant, to vulnerability. PRS technology manufacturer oversight would also be outsourced to the CPA of another country. Early consultation with potential PRS technology manufacturers has warned against the oversight of commercially sensitive technology manufacture by the CPA of another country.

72. Clearly Option 2 is the most expensive in terms of both upfront and recurring costs. In terms of delivering the functions required of a CPA, it is a low-risk option, however, since a separate government body which delivered all functions of the CPA in-house would provide a

comprehensive service. It may suffer from duplication of effort, however, as existing capabilities in other government departments are not leveraged under this option.

73. Option 4 is the lowest cost option. It carries significant risks in terms of service continuity in that it devolves virtually all CPA functions elsewhere in Government. This means that this option will be highly susceptible to retrenching of Departmental priorities across a wide range of Government partners. This option also runs the risk of significant cost escalation over time should partner Departments choose to charge “consultancy rates” for the provision of their services.

74. **The preferred option is therefore Option 5.** The amalgamated approach strikes a balance between the risk of a poorer service from outsourced capability and the cost savings inherent in outsourcing capability. The key difference between this option and other options such as Option 2 or Option 4 is that the less labour intensive functions, such as user management, are outsourced to OGDs whereas other more labour-intensive functions are retained in-house.

Risks and assumptions

75. A number of assumptions have been made in appraising the costs and benefits associated with different forms of establishing a Competent PRS Authority. The key risks and assumptions of the appraisal are discussed below in more detail.

76. *Costs of delivering CPA functions in other parts of government:* Where functions are carried out within the UK CPA under Option 2 but in other parts of government in Options 4 or 5, it is assumed in most cases that the average annual costs are the same. It could be argued that the costs of delivering the function within the UK CPA could become lower relative to other options due to the benefits of coordination with other parts of the UK CPA. Other government departments may also charge “consultancy fees” to the CPA. Equally, it could be argued that the costs of leveraging capability from other parts of government in Options 4 and 5 could cost less than under Option 2 as existing capability may deliver functions more efficiently. In the absence of conclusive evidence either way, it was assumed that the cost to the Exchequer would be the same, regardless of where these capabilities sit within government departments and agencies.

77. *Cost of designating another Member State’s CPA:* In the absence of any other Member State having developed a CPA it is not possible to estimate the fee that would be charged by another CPA. It is assumed that cost estimates should be at least as high as those made for UK estimates where these estimates represent marginal costs which would be incurred by the other MS’s CPA (e.g. key management and distribution, user and manufacturer oversight). The assumption was made that a premium between 0 and 50 per cent would be charged, with a best estimate of 25 per cent. This premium accounts for the fact that MSs may charge a “consultancy fee” to the UK for the services provided in an attempt to recover some of their sunk costs (e.g. POC-P infrastructure and CPA accommodation costs). In the absence of this 25 per cent premium, the NPV of Option 3 would be lower than the other options (-4.819m) and therefore could be an attractive option, although the commercial risks are still significant under this option. It is considered unlikely that another MS would not charge a premium over marginal costs, however, given the significant investment required to purchase a POC-P and the accompanying securing hosting infrastructure.

78. *Commitment from OGDs:* Full commitment from OGDs is assumed in outsourcing CPA functions in Options 4 and 5. Use of OGD capability, especially in times of fiscal austerity, could result in certain PRS functions being dropped in favour of internal priorities. This would affect the quality of service delivered to PRS users and manufacturers.

79. *Designation of PRS functions:* In Option 3 it is assumed that certain CPA functions are delegated to the CPA of another MS where delegation of these functions is not thought to damage national sovereignty. The assignment of functions in Table 1 follows initial consultation on which functions could be designated abroad. These will be the subject of consultation and more functions which in turn could affect the costs.

80. *Benefits of PRS technology to the user community:* The key benefits of PRS technology to the users of PRS lie in its increased resilience to spoofing and jamming and its availability in times of crisis as well as the possibility of interoperability with other GNSS technology. With this embryonic technology its benefits relative to GPS have yet to be proven. There is a significant risk that uptake of PRS technology will be low in the beginning. Thus, it could be envisaged that the role of the Competent PRS Authority in the early years would be to authorise the manufacture of PRS technology as the user community may remain small or non-existent. In that case the costs of running the CPA would be significantly reduced in all cases. The analysis undertaken here assumes a PRS user community from the outset in order to allow for a complete options analysis for the long-term. Similarly, this analysis makes the simplifying assumption that the costs pertaining to monitoring and managing users and manufacturers over time are constant over time. Although it is unlikely that this will be the case, as it is envisaged both groups will grow over time, in the absence of predictions as to the market size of PRS a constant, modest size was assumed. The results of the GNSS and PRS market study which is being conducted by the GSA, and which will become available during consultation, will provide further evidence on the likely size of the PRS market and on the uptake of PRS technology.

81. *First-mover advantage in the market for PRS:* The key assumption behind the benefits of PRS and, by association, the benefit of creating a Competent PRS Authority is that if the UK is one of the first countries to create a CPA that it will enjoy a first-mover advantage in the market for PRS technology. Quarterly briefing from the GNSS Security Board shows that other Member States are immature in terms of setting up their own CPAs. It is assumed the UK is well placed to take advantage of the market, having had a strong involvement in the development of PRS technology to date and playing a key role in piloting PRS technology and applications. There is the risk of over-estimating this potential benefit. It is not yet possible to envisage who the core suppliers of PRS technology manufacture will be. Further evidence will emerge during consultation stage on the progression of other MSs in creating CPAs, along with the success of UK manufacturers in the PRS technology pilots will shed further light on the likelihood of UK success in capturing a significant share of the market for PRS.

82. Annex 1

Functions of a Competent PRS Authority

The functions required of a Competent PRS Authority, as detailed in Article 5(4) and 5(5) of Decision 1104/2011/EU are detailed below.

CPA function (as in Articles 5(4) and 5(5) of Decision 1104	Task
1. Ensure compliance with the common minimum standards	Develop a compliance regime to assure compliance with the common minimum standards and take corrective action where instances of non-compliance are found within manufacturers or user communities
2. Grouping of users for the management of the PRS with the Global Security Monitoring Centre	Organisation of PRS user groups into wider communities with similar needs.
3. Determine and manage the PRS access rights for each group or user	Access rights for user groups and communities are overseen and managed centrally
4. Obtain the PRS keys and other related classified information from the GSMC	
5. Distribute PRS keys and other related classified information are distributed to users	
6. Manage the security of the receivers and associated classified technology and information and assess the risks	Oversee the security of the receivers and associated classified technology and information within user communities and periodically re-assess how user communities manage their equipment
7. Establish a point of contact for assisting as necessary in the reporting of detected potentially harmful electromagnetic interference affecting the PRS	Ensure that all relevant UK and EC agencies are notified of a relevant POC for reporting EM interference
8. Ensure that a body established on the territory of its Member State may only develop or manufacture PRS receivers or modules if such a body (a) has been duly authorised by the Security Accreditation Board in accordance with Article 11 (2) of Regulation (EU) No 912/2010; and (b) complies both with the decisions of the Security Accreditation Board and with Article 8 and point 2 of the Annex regarding the development and manufacture of PRS receivers or security modules, in so far as these relate to its activity.	Provide an evidence base against which the Security Accreditation Board can assess MS recommendations to authorise PRS manufacturers. Any authorisation provided needs to be reviewed at least every five years.
9. In the case of export outside the Union, act as an interface to the entities competent for export restrictions of relevant equipment, technology and software regarding the use, development and manufacturing of the PRS	Act as liaison between National Government and manufacturers who want to export PRS technology to third countries

Annex 2

Common Minimum Standards ***As extracted from the Annex to Decision 1104/2011/EU***

The common minimum standards to be complied with by the competent PRS authorities are set out in the Annex of the Decision 1104/2011. They relate to the use of PRS, the development and manufacture of PRS receivers or security modules and for export restrictions. These common minimum standards are described below.

The common minimum standards for the use of PRS cover the following areas:

- (i) PSR user group organisation;
- (ii) Definition and management of access rights for PRS users and user groups of PRS participants;
- (iii) Distribution of PRS keys and related classified information between the GSMC and the competent PRS authorities;
- (iv) Distribution of PRS keys and related classified information to the users;
- (v) Security management, including security incidents, and risk assessment for PRS receivers and associated classified technology and information;
- (vi) Reporting of detected potentially harmful electromagnetic interference affecting the PRS;
- (vii) Operational concepts and procedures for PRS receivers.

The common minimum standards for the development and manufacture of PRS receivers or security modules cover the following areas:

- (i) PRS user segment authorisation;
- (ii) Security of PRS receivers and PRS technology during research, development and manufacturing phases;
- (iii) PRS receiver and PRS technology integration;
- (iv) Protection profile for PRS receivers, security modules, and material using PRS technology

The common minimum standards for export restrictions cover the following areas:

- (i) Authorised PRS participants;
- (ii) Export of PRS-related material and technology.

The common minimum standards for the links between GSMC and the competent PRS authorities cover data and voice links.

Annex 3

Impact on sovereignty or wider national interests of other MS ownership of CPA functions

CPA function	Impact on sovereignty or wider national interests	Recommendation on outsourcing of function
1. Ensure compliance with the common minimum standards	The compliance function requires some form of oversight of both manufacturers and user communities. If the compliance function were outsourced to another MS it would require an acceptance of external scrutiny by a foreign government of certain functions of UK government, Critical National Infrastructure and hi tech manufacturing capability.	No
2. Grouping of users for the management of the PRS with the Galileo Security Monitoring Centre	One of the key benefits of PRS lies in the ability to sustain SatNav capability in times of crisis or in the event that open signals are unavailable. Outsourcing this function would require an acceptance that in a time of national crisis another MS government would determine / manage / control access to a potentially key emergency response capability	No
3. Determine and manage the PRS access rights for each group or user	One of the key benefits of PRS lies in the ability to sustain SatNav capability in times of crisis or in the event that open signals are unavailable. Outsourcing this function would require an acceptance that in a time of national crisis another MS government would determine / manage / control access to a potentially key emergency response capability	No
4. Obtain the PRS keys and other related classified information from the Galileo Security Monitoring Centre	Access to the PRS is dependent on obtaining the keys which enable the receivers to decode the encrypted signal. Outsourcing this function requires an acceptance that another MS would be responsible for obtaining these keys on behalf of the UK Government.	Yes
5. Distribute PRS keys and other related classified information to users	Once the classified encryption keys have been obtained from the Galileo Security Monitoring Centre they will need to be distributed to the UK's PRS user communities. Outsourcing this function requires acceptance that government representatives from another MS will assume this responsibility and may gain significant insight to the inner working of UK Government and critical national services	No
6. Manage the security of the receivers and associated classified technology and information and assess the risks	User communities will need to assure that receivers and associated technology are managed and effective measures set in place to guard against loss or damage in accordance with the requirements set out in the common minimum standards. Outsourcing this function requires acceptance that another MS government would be empowered to assess how UK entities safeguard crypto items and other security assets.	No

7. Establish a point of contact for assisting as necessary in the reporting of detected potentially harmful electromagnetic interference affecting the PRS	This requirement cannot be outsourced to another MS as the point of contact needs to be established within the UK.	No
8. Ensure that a body established on the territory of its Member State may only develop or manufacture PRS receivers or modules if such a body (a) has been duly authorised by the Security Accreditation Board in accordance with Article 11 (2) of Regulation (EU) No 912/2010; and (b) complies both with the decisions of the Security Accreditation Board and with Article 8 and point 2 of the Annex regarding the development and manufacture of PRS receivers or security modules, in so far as these relate to its activity.	This obligation requires manufacturers of PRS technology to undergo some form of assessment to demonstrate that they can be authorised to manufacture classified technology. Outsourcing this function requires an acceptance that representatives from other MSs will scrutinise the protective security measures and hi tech manufacturing processes of UK companies, many of which are considered leaders in the field.	Yes
9. In the case of export outside the Union, act as an interface to the entities competent for export restrictions of relevant equipment, technology and software regarding the use, development and manufacturing of the PRS	This obligation requires member states to provide advice on export controls via the relevant National Authorities. It would be difficult to outsource this role to another MS.	No

Annex 4

Accommodation requirements for UK CPA

STAFF

Estimate of number of FTE staff in UK CPA office under Options 1 – 5. These FTE staff numbers and the assumptions associated with them are explained in more detail in Table 3.

	Option 1: Do nothing	Option 2: New government office	Option 3: De minimus	Option 4: Federated approach	Option 5: Amalgamated approach
Managing users	0	0.5	0	0.5	0.5
Oversight of manufacturers	0	3	0	0.5	3
Export control	0	0.3	0	0.1	0.1
Total FTEs in each option	0	3.8	0	1.1	3.6
Workstation cost (based on internal BIS estimate of £5,000 per workstation in London)	£0	£19,000	£0	£5,500	£18,000

LOCATION

Existing UKSA offices (BIS) in London (the Swindon site, not being a secure site, is not considered at this point).

