

Annex I

ACCESS & CONTACT GRIDS

CONTRACTOR'S CONTACTS		
Project Manager <i>Set-up and management of the connection</i>	Name	
	Function	
	Telephone	
	Email	
Contact person/team <i>Incident handling during working hours (including operational and security incidents)</i>	Name	
	Function	
	Telephone	
	Email	
Contact person/team <i>Incident handling outside working hours (including operational and security incidents)</i>	Name	
	Function	
	Telephone	
	Email	
Escalation procedure	Name	
	Function	

<i>Incident handling (including operational and security incidents)</i>	Telephone	
	Email	

Requested token and authorized staff			
<i>Typically EMSA will provide a single token. Should the contractor require additional tokens, it should be reflected on the table below. Additional tokens will only be provided under exceptional circumstances with proper justification.</i>			
Token number		Member staff and role	
		Member staff and role	
		Member staff and role	

EMSA'S CONTACTS		
Project Officer <i>Set-up and management of the connection</i>	Name	
	Function	
	Telephone	
	Email	
ICT Service Desk <i>Set-up and management of the connection</i>	Name	Roar Fondse
	Function	ICT Service Desk
	Telephone	+351 21 1209 321
	Email	ICT.servicedesk@emsa.europa.eu
Contact person/team <i>Incident handling 24/7 (including operational and security incident)</i>	Name	Maritime Support Service (MSS)
	Function	24/7 Maritime Support
	Telephone	+351 21 1209 415
	Email	maritimesupportservices@emsa.europa.eu

INBOUND NETWORK ACCESS TO EMSA'S ICT RESOURCES

For each resource, indicate the services required to perform the tasks described in the specific agreement.
Use one line per service even if several services are hosted on the same server.

Inbound Connections to EMSA's ICT Resources (Normally completed by EMSA PO with the Input from the contractor)											
ID	Application (and DC Rfc number if applicable)	Associated Application Data Assets (e.g. SSN ship coordinates, user database)	Component (Oracle, WebLogic, Linux account, etc.)	IP Address or NAME (Name or DNS Name or Generic service)	Location (DMZ or Data Centre or EMSA Intranet)	Service Port ¹	Port Description ²	Access Starting Date ³	Latest End Date ⁴	Description	Authenti- cation Type
1											
2											
3											

¹ Application port number (ex: TCP 80, TCP 443, TCP 2010 ...). UDP based applications protocols are not permitted.

² Application (protocol) name (ex: HTTP, HTTPS ...). For custom protocols, enter the name of the protocol (if exist) or the name of the application accessed through this protocol.

³ Access to the specific resource will be **opened** as from this day on.

⁴ Access to the specific resource will be **blocked** as from this day on

Inbound Connections to EMSA's ICT Resources
(Normally completed by EMSA PO with the Input from the contractor)

ID	Application (and DC Rfc number if applicable)	Associated Application Data Assets (e.g. SSN ship coordinates, user database)	Component (Oracle, WebLogic, Linux account, etc.)	IP Address or NAME (Name or DNS Name or Generic service)	Location (DMZ or Data Centre or EMSA Intranet)	Service Port¹	Port Description²	Access Starting Date³	Latest End Date⁴	Description	Authenti- cation Type
4											
5											
6											
7											
8											

CONTRACTOR'S OUTBOUND ACCESS NETWORK AND ICT RESOURCES USED FOR THE ACCESS TO EMSA'S ICT RESOURCES

Data Transmission Network <i>(This information will be used for compliance checking and troubleshooting purposes)</i>	
Inbound Internet Link Bandwidth <i>("P" for primary connection and "B" for back-up connection)</i>	
Outbound Internet Link Bandwidth <i>("P" for primary connection and "B" for back-up connection)</i>	
Operational System where VPN client will be installed <i>(Specify if Windows XP, Windows Vista or Windows 7)</i>	