SCHEDULE 2.1 (SERVICES DESCRIPTION)

PART 13 – TECHNICAL

ANNEX M - TECHNICAL & APPLICATIONS

APPENDIX 3 - PATCHING REQUIREMENTS AND TIMESCALES

1 DEFINITIONS

1.1 In this Part 13 of Schedule 2.1 the following definitions shall apply:

Release Programme	the programme of how frequently the Authority performs Major Releases;

2 PATCHING REQUIREMENTS AND TIMESCALES

2.1 The Contractor shall maintain the ICT Hardware and Software that is used to deliver the Services for the Authority to an appropriate level to adhere to the Authority and Accreditor expectations and needs.

2.2 Unless otherwise specified by other Authority sources responsible for specifying a timescale for patch implementation (for example, MODCERTS), timescales for Patches are to be applied as follows:

PATCHING GROUP	TIMESCALES
Enterprise Application Patching (for example, JPA, CASS, CAPS, StratMI, and Oracle RDBMS)	'Cyber Incident Response Team' Patches are to be deployed within 10 Working Days of notification, unless agreed otherwise.
	Security Patches are to be deployed within 10 Working Days of release, unless agreed otherwise by the Authority (Tech Assurance).
	Routine Patches are to be deployed in line with the Release Programme.
	Enterprise Application Patches are to be sourced directly from the third party vendor.
Desktop Applications (for example, Microsoft Windows Client, Microsoft Office, and Adobe Reader)	'Cyber Incident Response Team' Patches are to be deployed within 5 Working Days of notification, unless agreed otherwise by the Authority (Tech Assurance).
	Security Patches are to be deployed within 10 Working Days of release to DOBUS, unless agreed otherwise by the Authority (Tech Assurance).
	Routine Patches are to be deployed within 30 Working Days of release to DOBUS, unless agreed otherwise by the Authority (Tech Assurance).
	Desktop Applications are to be sourced from DOBUS (unless otherwise agreed).
WINTEL Servers (for example, Microsoft	'Cyber Incident Response Team' Patches are to be deployed within 10 Working Days of notification, unless agreed otherwise by the Authority (AH Tech Assurance).

PATCHING GROUP	TIMESCALES
Windows Server, IIS, and CITRIX)	Security Patches are to be deployed within 15 Working Days of release to DOBUS, unless agreed otherwise by the Authority (Tech Assurance).
	Routine Patches are to be deployed in line with Release Programme.
	WINTEL Server Patches are to be sourced from DOBUS (unless otherwise agreed).
Hardware Platforms (for example, Network firewalls, Load Balancers, Routers, Switches, Appliances, Exadata, OEL, and AIX)	'Cyber Incident Response Team' Patches are to be deployed within 10 Working Days of notification, unless agreed otherwise by the Authority (Tech Assurance).
	Security Patches are to be deployed within 30 Working Days of release to DOBUS, unless agreed otherwise by the Authority (Tech Assurance).
	Where feasible, desirable and dependent on the criticality, routine Patches are to be deployed in line with Release Programme, to avoid out of release testing impact..
	Hardware platform Patches are to be sourced from DOBUS (unless otherwise agreed).
Anti-Virus Updates - Virus Database	Anti-Virus Database definition updates are to be hourly.
	CIRT definition Updates are to be within 4 hours (during a Working Day) of notification, unless agreed otherwise by the Authority (Tech Assurance).
Anti-Virus Updates - Core Software	Anti-Virus Software Updates are to be monthly, unless agreed otherwise by the Authority (Tech Assurance).
	'Cyber Incident Response Team' Updates to the core software is to be within 5 Working Days of notification, unless agreed otherwise by the Authority (Tech Assurance).
	Sourced from DOBUS (unless agreed otherwise by the Authority (Tech Assurance)).

3 SERVICE PACKS

For items defined or designated as being a service pack by the Third Party Software vendor would be treated as change and built into a release

4 IMPLEMENTATION IMPACT

4.1 All Patches and upgrades to Hardware or Software are to be impact assessed and tested before release to the Production Environment, in line with the Change Control Procedure.

4.2 The Contractor shall notify the Authority (Technical Assurance) of any issues arising out of such Patches and hardware upgrades as soon as the Contractor becomes aware.