SCHEDULE 11
SECURITY

1. General

1.1 The requirements set out in this Schedule 11 (Security) relate to the steady state provision of the Services, and not to any period of Transition prior to TORD.

1.2 The CONTRACTOR will have overall responsibility for achieving and maintaining security accreditation of the Services, defined as the continued security approval for live operations as granted by the AUTHORITY and the nominated Accreditor. However, accreditation will rely upon the security of the Hosting Services delivered by the Government Gateway Hosting Services Provider through the transition of the Hosting Services into this Agreement.

1.3 For the avoidance of doubt, the responsibility for achieving and maintaining security accreditation includes:

(A) ensuring that agreed security policies, as defined in the existing Risk Management Accreditation Document Sets (RMADS) relating to the Gateway Technical Infrastructure managed by the CONTRACTOR, are enforced;

(B) maintenance of security documentation;

(C) managing the secure delivery of the Services including the process of rolling out new Service Builds to AUTHORITY's Customers;

(D) managing security in the support processes relating to the Services; and

(E) managing security in the development of new elements of the Services, in terms of the development process itself, the security of the new development, and the impact on the Gateway and the existing Services.

1.4 Notwithstanding any other provision of Schedule 18 (Approved Subcontractors) and for the avoidance of doubt, each obligation placed on the CONTRACTOR by the terms of this Schedule 11 (Security) shall be deemed to be an obligation on the CONTRACTOR to procure that any Subcontractor, agent or other third party under the control of the CONTRACTOR complies with such obligation.

1.5 The AUTHORITY will be responsible for classifying the AUTHORITY's Data for security purposes.

1.6 The AUTHORITY will be responsible for providing to the CONTRACTOR copies of all security policy documentation where these are not available to the CONTRACTOR via the internet or the parts of the AUTHORITY's or UK Government's intranet to which the CONTRACTOR has access.

2. Basis for Security Requirements in Government Gateway Services

2.1 The CONTRACTOR shall comply with the security requirements set out in the version of the RMADS applying to the Gateway that is current at the date of signature of this Agreement by the CONTRACTOR. Any subsequent changes to the agreed security

measures and responsibilities must be agreed with the AUTHORITY, the nominated Accreditor and the CONTRACTOR.

2.2 The CONTRACTOR shall develop and agree security policy, standards and procedures relating to the delivery, support and development of the Services, and shall be responsible for implementing the measures contained therein.

3. **Protective Markings and Clearances**

3.1 All documentation relating to the design, build and/or operation of the Gateway shall be treated as RESTRICTED save that any items containing material, the release of which could significantly compromise the security of the Gateway, shall be treated as CONFIDENTIAL.

3.2 The CONTRACTOR shall treat any information relating to Security Incidents and suspected Security Incidents as, at least, RESTRICTED.

3.3 The CONTRACTOR shall, with the reasonable assistance of the AUTHORITY, obtain all necessary CONTRACTOR (including Subcontractor personnel and agents) security clearances in line with the following requirements:

(A) the minimum level of security clearance for any user access to the Gateway Technical Infrastructure is Basic Check ("BC");

(B) the minimum level of security clearance for system administrative access to the Gateway Technical Infrastructure is Security Check ("SC"); and

(C) the minimum level of security clearance for any user to configure the Gateway Technical Infrastructure is SC.

3.4 The requirements stated at paragraphs 3.3(A) and 3.3(B) above shall also apply to any contractor to the CONTRACTOR (including the CONTRACTOR's Personnel) working on temporary or short-term assignments or ad hoc projects.

3.5 The requirements stated at paragraphs 3.3(A) and 3.3(B) above shall not apply when an uncleared individual is closely supervised at all times by a member of the CONTRACTOR Personnel or the AUTHORITY's personnel carrying the appropriate level of security clearance.

3.6 CONTRACTOR Personnel required to handle protectively marked Data (as defined by the Protective Marking Scheme) shall be subject to security clearance to a level commensurate with that Data.

3.7 Any security clearances obtained by the CONTRACTOR shall be notified to and agreed by the AUTHORITY's security branch from time to time.

3.8 Access by Subcontractors' maintenance staff must be controlled by the CONTRACTOR either by ensuring that the relevant Subcontractor's representative is security cleared as described in paragraph 3.3 above or is accompanied as described in paragraph 3.5 above.

3.9 The CONTRACTOR and all of its Subcontractors must have a security awareness programme in place to make certain that all CONTRACTOR Personnel who may come in to contact with All Material are aware of the need to preserve its security.

3.10 The CONTRACTOR and all of its Subcontractors must have a security training programme in place for CONTRACTOR Personnel with specific security responsibilities.

4. **Asset Management (Security)**

4.1 The CONTRACTOR shall be responsible for maintaining control of access including access by Subcontractors, agents and third parties to All Material under the control of the CONTRACTOR, including where relevant, at any CONTRACTOR Premises employed in the delivery of the Services.

4.2 Information under the control of the CONTRACTOR shall be marked in accordance with the Protective Marking Scheme and the Security Aspects Letter issued by the AUTHORITY in accordance with the requirements of the Manual of Protective Security.

4.3 Organisations to whom information is to be sent by the CONTRACTOR shall be informed by the CONTRACTOR of the protective marking associated with that information to ensure that it will be handled by personnel with suitable security clearance corresponding to the protective marking.

4.4 Formal dispatch records or logs must be kept by the CONTRACTOR where Data and documents are sent by the CONTRACTOR to other organisations.

4.5 Only data communications links approved by the AUTHORITY may be used to transmit All Material owned by the AUTHORITY.

4.6 On the formal written request of the AUTHORITY, the CONTRACTOR must remove all or any combination of All Material to archive storage or ensure that the material is securely destroyed when no longer required for use in the Services, provided that such removal shall not adversely impact the delivery of the Services.

4.7 The CONTRACTOR shall take all reasonable steps to prevent the theft, unauthorised alteration, substitution or destruction of All Material owned by the AUTHORITY under the control of the CONTRACTOR.

4.8 The CONTRACTOR must, prior to the repair or disposal of any system component or hardware holding any information, Government code or All Material used in the provision of the Services securely cleanse the contents of the system component or hardware using processes agreed with the AUTHORITY. On completion of the cleansing process a completion certificate shall be issued by the CONTRACTOR to the AUTHORITY certifying that the system component or hardware has been securely cleansed. During the disposal process the CONTRACTOR shall maintain an appropriate level of security for the contents of the system component or hardware being cleansed.

4.9 During the term of the Services, any system component or hardware, including any respective part of All Material and/or Data, decommissioned or disposed of during the

term of the Services must also be disposed of in accordance with Government policy and with the agreement of the Accreditor.

4.10 At the end the Services or following any period of post-termination support at the request of the AUTHORITY, the CONTRACTOR shall draw up and agree with the AUTHORITY a plan to ensure that All Material, Data, system components and hardware to be disposed of by the CONTRACTOR are disposed of in accordance with Government policy and with the agreement of the Accreditor. Where there is List X sponsorship in relation to the Services, that shall remain in force until such time as the AUTHORITY agrees that it is no longer required.

4.11 CONTRACTOR security personnel involved with the provision of the Services shall use reasonable endeavours to maintain awareness of changes in threats and vulnerabilities to the Services. The CONTRACTOR must put in place a mechanism to recognise a temporary increase in level of threat and procedures to raise the state of vigilance if required. The AUTHORITY is responsible for ensuring that notifications of threats to the Services are transmitted to the CONTRACTOR to enable the CONTRACTOR to raise the state of vigilance. The CONTRACTOR is responsible for notifying the AUTHORITY of any circumstances which could give rise to a change in the local alert state.

4.12 Any amendment made by the CONTRACTOR to any component of All Material must be made by copying the specific component and making the amendments to the copy.

4.13 The CONTRACTOR shall ensure that all print-outs generated by the CONTRACTOR in relation to the provision of the Services that have been received by a print server are complete.

5. **Standards and Policy**

5.1 The CONTRACTOR shall ensure that the Services provided shall comply with all relevant aspects of the requirements of referenced documents, including but not limited to the following documents as amended or updated from time to time:

(A) Manual of Protective Security, associated HMG Information Security (Infosec) Standards and CESG publications (including Electronic Information Processing Security Notices);

(B) the AUTHORITY's security policy (ukonline programme information security policy);

(C) the AUTHORITY's IT security manual (Cabinet Office Security Policy), as issued by the Cabinet Office Security Policy Division;

(D) relevant security policies and practices arising from external connections necessary for the provision of the Gateway Services;

(E) e-Government Strategic Framework; and

(F) e-Government Interoperability Framework and associated CSIA publications.

5.2 In the delivery of the Services, the CONTRACTOR shall comply with the principles of BS7799 Part 2-2005 (ISO-27001-2005).

6. **Security Policy**

6.1 The CONTRACTOR shall maintain the components of the security documentation necessary for the security accreditation of all relevant systems, whose use and ongoing development in each case shall be governed by the following principles:

(A) the CONTRACTOR shall be responsible for compiling and gaining agreement for any changed or new security documentation required as a result of changed or new components of the Services;

(B) the security documentation shall specify the security policies, risks, measures and procedures required;

(C) the security documentation remains the property of the AUTHORITY. All rights and title to, and interests in, the security documentation, including Intellectual Property Rights shall vest automatically with the AUTHORITY;

(D) changes to the security documentation shall be discussed and agreed with the AUTHORITY and with the nominated Accreditor for the Government Gateway Services;

(E) the security documentation shall comply with the AUTHORITY's security policy but the security policies, risks, measures and procedures set out in the security documentation shall not compromise the Service Levels set out in Schedule 4 (KPIs, Service Levels and Service Credits) for the Services;

(F) the security documentation shall include security operating procedures to ensure that all Security Incidents are logged and dealt with. This shall include an analysis component which addresses the lessons to be learned and provides for those lessons to be put into practice;

(G) Security Incidents affecting the Services must be reported in accordance with the HMG Unified Incident Reporting and Alert Scheme (UNIRAS);

(H) the security documentation shall include a Security Incident response plan for the Services, including a forensic readiness plan;

(I) any Changes to the security documentation or the counter measures contained therein which Change the obligations on the CONTRACTOR shall be subject to the Change Control Procedure;

(J) the CONTRACTOR shall be responsible for producing and maintaining complete and up-to-date security documentation, and for working with the AUTHORITY to achieve the approval of the security documentation in accordance with the review and approval procedure;

(K) the CONTRACTOR shall be responsible for ensuring that the Gateway-related operations at the Data Centre and at other CONTRACTOR Premises used by the CONTRACTOR to deliver, develop and support the Services comply with

the relevant CONTRACTOR requirements set out in the approved security documentation and shall ensure that all related systems used by the Subcontractors in the delivery of the Services also comply with the relevant Subcontractor requirements set out in the approved security documentation;

(L) the CONTRACTOR shall comply with the relevant approved security documentation (of which it has been notified) in respect of all other systems and all business processes under the security control of the AUTHORITY or any Subcontractors, agents and third parties that the CONTRACTOR has or requires access to. Where such security documentation is not notified to the CONTRACTOR until after signature of this Agreement and compliance with such security documentation affects the CONTRACTOR's ability to provide the Services or increases the CONTRACTOR's costs of providing the Services then any compliance with such security documentation shall be subject to the Change Control Procedure; and

(M) the AUTHORITY shall procure that all of its contractors (other than the CONTRACTOR, its Subcontractors and agents) providing related services also comply, where necessary, with the agreed site security procedures.

6.2 The CONTRACTOR's security policy and procedures shall be consistent with the AUTHORITY's security policies and procedures, as laid down in the AUTHORITY's security policy as they pertain to the Services.

6.3 In addition to complying with the provisions of this Schedule 11 (Security) as at the Commencement Date the CONTRACTOR shall comply with all further security requirements that are or may from time to time be required by the AUTHORITY to be enforced at the AUTHORITY Premises or CONTRACTOR Premises to and from which the Services are or are to be provided. Where the enforcement of such further security requirements affects the CONTRACTOR's ability to provide the Services or increases the CONTRACTOR's costs of providing the Services to or from the AUTHORITY or CONTRACTOR Premises, then compliance with such further security requirements shall be subject to the Change Control Procedure.

6.4 Where the CONTRACTOR wishes to provide all or part of the Services from an offshore location then further requirements may apply, at the discretion of the Accreditor and other relevant security agencies. Meeting the additional requirements shall be the responsibility of the CONTRACTOR.

6.5 The CONTRACTOR shall ensure that any communication links required for the provision of the Services are secured according to Government guidelines, provided that any additional cost of doing so is subject to the Change Control Procedure.

7. **Organisation**

7.1 The CONTRACTOR shall implement a Security Management process for the delivery, support and development of the Services which is compliant with BS7799-2:2005 (ISO-27001-2005). A Chief Security Manager shall be identified to be responsible for day to day security implementation, audit and security plans.

7.2 Access by Subcontractors to All Material owned by the AUTHORITY and in the possession and control of the CONTRACTOR and access to any related equipment, media or other devices must be strictly limited and controlled by the CONTRACTOR.

7.3 Where CONTRACTOR Personnel need unsupervised access to All Material owned by the AUTHORITY the CONTRACTOR will arrange for appropriate security clearance as set out in paragraph 3.3 above.

8. **Security Incidents**

8.1 The CONTRACTOR shall ensure that all Security Incidents are reported in line with UNIRAS or CINRAS as appropriate, and that suspected security weaknesses of which it is aware are dealt with promptly and that there is an action plan agreed with the AUTHORITY to stop any reoccurrence.

8.2 The CONTRACTOR shall maintain adequate records and facilitate inspections to enable the investigation of Security Incidents.

9. **Physical and Environmental Security**

9.1 The CONTRACTOR shall take all reasonable steps to prevent the theft or unauthorised alteration, substitution or destruction of All Material owned by the AUTHORITY and held under the control of the CONTRACTOR.

9.2 The AUTHORITY shall take all reasonable steps to maintain the physical security of its own systems and/or equipment on AUTHORITY Premises.

9.3 The AUTHORITY shall be responsible for establishing a process for identifying and maintaining the list of AUTHORITY Employees authorised to access the Data Centre.

9.4 Changes in Government policy affecting the security requirements for the service, as they are made available to the AUTHORITY, shall be made known to the CONTRACTOR.

9.5 The AUTHORITY shall permit and procure reasonable access to AUTHORITY Premises for CONTRACTOR Personnel for the purpose of performing the CONTRACTOR's obligations in relation to the delivery of the Services.

9.6 The CONTRACTOR shall ensure that the following requirements are met at any CONTRACTOR Premises used or to be used in the delivery, development and support of the Services:

(A) the CONTRACTOR Premises, including the Data Centre, must provide a degree of resistance to a forced attack including without limitation an appropriate level of physical outside security (such as perimeter fencing) and appropriate doors, locks, windows and hinges;

(B) access to the CONTRACTOR Premises must be restricted to authorised personnel. This requires the entrance to such CONTRACTOR Premises being appropriately secured and for it to be possible to identify those who have access;

(C) visitors must be identifiable as visitors and escorted whilst they are on such CONTRACTOR Premises;

(D) the entrances to and exits from the CONTRACTOR Premises must be supervised or have approved electronic controls in place;

(E) an alarm system capable of raising an external alarm must be installed. This alarm must trigger if an attempt is made to disable it;

(F) the security of the Data Centre must not be the responsibility of only a single security guard, unless that single guard can view CCTV of the Data Centre;

(G) a mechanism must be in place to recognise a temporary increase in level of threat and procedures to raise the state of vigilance if required;

(H) deliveries will be subject to agreed delivery procedures and physically secured away from critical work areas until they have been inspected and it is confirmed that they do not prevent a physical security threat;

(I) the Gateway Technical Infrastructure should be sited in such a manner as to minimise the risk of accidental leakage or ingress of water causing damage of any kind;

(J) the CONTRACTOR Premises, including the Data Centre, must be sited in areas that are not prone to natural and identifiable man made disasters;

(K) the CONTRACTOR Premises, including the Data Centre, must be protected against lightning strikes; and

(L) power equipment must be installed according to relevant regulations.

9.7 The relevant Government standards (primarily the Manual of Protective Security) shall apply to all CONTRACTOR Premises holding protectively marked material.

9.8 All CONTRACTOR Premises holding material protectively marked CONFIDENTIAL must be approved List X Premises.

9.9 All CONTRACTOR Premises holding non-protectively marked material related to the delivery of the Services must follow Best Practice.

10. **Communications and Operations Management**

10.1 The CONTRACTOR must implement agreed technical measures and must define and agree during Transition supporting procedures which will allow back-ups to be taken in accordance with an agreed Risk Management and Accreditation Documentation Sets (RMADS), and which will ensure that:

(A) back-ups are stored in an environment whose security is appropriate for the protective marking of the back-ups;

(B) All Material and Data are backed up to ensure that they are protected against the failure of any single hardware device;

(C) following a disk crash or a software error, it would be possible to re-create Data lost since the previous back-up;

(D) the back-up and restore procedures are tested annually to ensure that systems and Data can be recovered successfully and that Data integrity is maintained following an error; and

(E) all full back-ups can be stored for a minimum of one (1) year.

11. **Access Control and Malicious Software**

11.1 The CONTRACTOR must during Transition implement agreed technical measures and must define and agree supporting procedures which will ensure that:

(A) only users authorised by the AUTHORITY have access to the Gateway Technical Infrastructure;

(B) access to Data is controlled by the designated Data owners whose identity will be notified by the AUTHORITY to the CONTRACTOR from time to time;

(C) there is strict logical and physical separation of All Material owned by the AUTHORITY from information held for any other client of the CONTRACTOR. The logical separation must be at least to a level compliant with the Manual of Protective Security and its component elements including HMG Infosec Standards and CESG publications;

(D) CONTRACTOR Personnel are given the minimum possible access rights to All Material owned by the AUTHORITY that still allows them to carry out their duties effectively;

(E) unattended workstations within the Data Centre are protected against use by an unauthorised person;

(F) the use of privileged functions (access to documentation relating to the design, build and/or operation of the Gateway and system administrative access) is controlled and used by SC cleared staff only. For the avoidance of doubt, due to the timescales of the provision of the Services, the CONTRACTOR must at least have Key Personnel in the SC process on the signing of this Schedule 11 (Security) and have obtained BC clearance and undergone a counter terrorism check (CTC);

(G) the Gateway is monitored constantly using appropriate security software for activity which could potentially damage it, and all relevant equipment used to support, deliver and develop the Services has appropriate anti-virus software on all relevant points of entry;

(H) the potential for malicious damage to the Gateway is minimised;

(I) any malicious software is identified, isolated, and removed;

(J) anti-virus software is regularly updated on a not less than daily basis to ensure implementation of all patches;

(K) UNIRAS briefings and alerts are monitored for information that pertains to the software and hardware used in the provision of the Services, any measures (other than the updating of virus information libraries) to be implemented through the Change Control Procedure;

(L) network security is compliant with HMG Infosec policy;

(M) only data communications links approved by the AUTHORITY (which for the avoidance of doubt may approve communication links which do not comply with any or all of the remaining provisions of this Schedule 11 (Security)) have access to All Material owned by the AUTHORITY;

(N) all entities which connect to the Gateway are identified and authenticated using appropriate methods;

(O) no additional links that may grant access to All Material owned by the AUTHORITY are introduced without the prior written approval of the AUTHORITY;

(P) connections to the Gateway are terminated when no longer required;

(Q) information that could be exploited to gain access to end systems (e.g. passwords, network addresses) is afforded an appropriate level of protection;

(R) unauthorised access to All Material and the Gateway Technical Infrastructure from remote access ports is prevented;

(S) unauthorised access from public networks is prevented. All access must be authorised access in line with HMG Infosec policy;

(T) access to all network diagnostic and control equipment is restricted to authorised personnel and usage logs are maintained; and

(U) access by maintenance staff is controlled either by ensuring that the relevant individual is security cleared as described in paragraphs 3.3 and 3.4 above or is accompanied as described in paragraph 3.5 above and the CONTRACTOR will notify the Accreditor of, and obtain agreement for, all proposals for remote maintenance and diagnostics.

12. **System Development and Maintenance**

12.1 The CONTRACTOR must during Transition implement technical measures agreed with the AUTHORITY and must define and agree with the AUTHORITY supporting procedures which will ensure that:

(A) all updates and patches to the standard application suite on the Gateway Technical Infrastructure are implemented, within an agreed timescale, in accordance with the Change Control Procedure and such updates and patches may be subject to audit; and

(B) CONTRACTOR security personnel involved with the provision of the Services use all reasonable endeavours to maintain awareness of changes in threats and vulnerabilities to the Services.

13. **IT Service Continuity Management**

13.1 The CONTRACTOR must implement technical measures agreed with the AUTHORITY and must define and agree with the AUTHORITY supporting procedures which will ensure that:

(A) Subcontractors providing network services are contractually obliged to provide a pre-determined minimum service level in accordance with the Services;

(B) alternative sources of input and output media are available if required;

(C) appropriate specialist advice is sought on identifying any vulnerable areas within each CONTRACTOR Premises. This will be the function of the Accreditor; and

(D) an uninterruptible power supply supported by alternative generated power is implemented to minimise the impact of a power failure.

14. **Emergency Response**

14.1 The CONTRACTOR must implement emergency response procedures to ensure:

(A) there is a fire prevention programme in place. If a fire occurs, procedures or physical safeguards must be in place to:

(1) detect the fire at an early stage and raise the alarm;

(2) safely evacuate all personnel; and

(3) minimise the spread of the fire;

(B) all relevant CONTRACTOR Personnel are informed of the information they will attempt to gather if a bomb warning is received. CONTRACTOR Personnel must be made aware of the actions they must take during a bomb warning;

(C) all relevant CONTRACTOR Personnel are aware of the actions they must take, should a suspect package be discovered; and

(D) All Material is secured prior to any evacuation, when it is possible to do so without increasing the risk to personnel safety.

15. **Compliance**

15.1 The security functionality and procedures defined above will be covered by a final security acceptance test prior to the Transfer of Responsibility Date. The planning, reviewing and performance of the final security acceptance test shall be undertaken in accordance with Schedule 10 (Acceptance).

15.2 All software, including updates and new versions, must undergo a series of security tests which shall count towards the granting of security approval to operate. For the avoidance of doubt, this encompasses any application level IT Health Checks required by the Accreditor.

15.3 The AUTHORITY shall be responsible for the costs of any additional health checks requested by the Accreditor arising from the acceptance test specified in paragraph 15.1 above.

15.4 Subject to paragraph 15.3 above, the CONTRACTOR shall be responsible for maintaining formal security accreditation for the operation of the Services, including such approvals as may be required for external connectivity.

15.5 Security policy and Documentation must be compliant with Government policy and the guidelines as described in this Schedule 11 (Security).

15.6 Security Management must be compliant with BS7799 Part 2-2005 (ISO-27001-2005).

15.7 Security Incident reporting timescales and approach shall, at all times, be consistent with the requirements of UNIRAS or CINRAS as appropriate.

15.8 The AUTHORITY must have the right to conduct unannounced but authorised inspections of the CONTRACTOR Premises hosting the Gateway, including the Data Centre and any support centre, and IT systems to ensure that the conditions of this Schedule 11 (Security) are being fulfilled. The CONTRACTOR may prevent access to the CONTRACTOR Premises and systems for the purposes of an unannounced inspection only for a time period reasonably necessary to authenticate the identity of the authorised personnel conducting the inspection.

15.9 The CONTRACTOR must during Transition implement technical measures agreed with the AUTHORITY and must define and agree with the AUTHORITY supporting procedures which will ensure that:

(A) it is possible to account for all actions that affect the Gateway and to have standard logging information for servers in the Gateway Technical Infrastructure;

(B) it is possible to account for each occasion when the Gateway is accessed;

(C) the log of the access to the Gateway is retained, in a secure manner, for at least six (6) months to allow investigations to be carried out where necessary;

(D) all suspected or detected attempts to breach security are investigated and reported to the AUTHORITY;

(E) a full record of all work conducted by software and hardware maintenance engineers is maintained;

(F) auditing and accounting is equivalent to “partial” as defined in HMG Infosec Standards;

(G) all audit logs are stored for at least six (6) months; and

(H) the secure operating procedures contain procedures to ensure compliance with relevant statutory and contractual security requirements, and with physical, procedural and technical countermeasures.

16. **Acceptance and Security Policy**

16.1 Upon the written request of the AUTHORITY, the CONTRACTOR shall submit a completed and signed copy of the form set out below to the AUTHORITY in order to provide documentary evidence to the Government security services of the CONTRACTOR's acknowledgement of, and compliance with, its obligations with regard to Protectively Marked Documents.

Accountability for Government security documentation

I / We the undersigned agree to protect the Government security documents referred to in this Schedule 11.

All security documents shall be locked away in a secure cabinet when not in use, and only used by CONTRACTOR Personnel with a minimum of Basic Check security clearance. The documents are provided for a specific contractual purpose and must be returned to the AUTHORITY on the termination of this Schedule 11 or upon request by the AUTHORITY.

Signature…….

Name ……

CONTRACTOR Name……

Date……..